aws

Panduan Pengguna ONTAP

fsX untuk ONTAP

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

fsX untuk ONTAP: Panduan Pengguna ONTAP

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang menghina atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan kekayaan masing-masing pemiliknya, yang mungkin atau mungkin tidak berafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu Amazon FSx untuk NetApp ONTAP?

Amazon FSx untuk NetApp ONTAP adalah layanan yang dikelola sepenuhnya yang menyediakan penyimpanan file yang sangat andal, terukur, berkinerja tinggi, dan kaya fitur yang dibangun di atas sistem file ONTAP yang populer. NetApp FSx untuk ONTAP menggabungkan fitur, kinerja, kemampuan, dan operasi API yang sudah dikenal dari sistem NetApp file dengan kelincahan, skalabilitas, dan kesederhanaan yang dikelola sepenuhnya. Layanan AWS

FSx untuk ONTAP menyediakan penyimpanan file bersama yang kaya fitur, cepat, dan fleksibel yang dapat diakses secara luas dari instance komputasi Linux, Windows, dan macOS yang berjalan di dalam atau di tempat. AWS FSx untuk ONTAP menawarkan penyimpanan solid state drive (SSD) berkinerja tinggi dengan latensi submilidetik. Dengan FSx untuk ONTAP, Anda dapat mencapai tingkat kinerja SSD untuk beban kerja Anda sambil membayar penyimpanan SSD hanya untuk sebagian kecil dari data Anda.

Mengelola data Anda dengan FSx untuk ONTAP lebih mudah karena Anda dapat memotret, mengkloning, dan mereplikasi file Anda dengan mengklik tombol. Selain itu, FSx untuk ONTAP secara otomatis meningkatkan data Anda ke penyimpanan elastis berbiaya lebih rendah, sehingga mengurangi kebutuhan Anda untuk menyediakan atau mengelola kapasitas.

FSx untuk ONTAP juga menyediakan penyimpanan yang sangat tersedia dan tahan lama dengan cadangan yang dikelola sepenuhnya dan dukungan untuk pemulihan bencana lintas wilayah. Untuk membuatnya lebih mudah untuk melindungi dan mengamankan data Anda, fsX untuk ONTAP mendukung keamanan data populer dan aplikasi antivirus.

Bagi pelanggan yang menggunakan NetApp ONTAP lokal, fsX untuk ONTAP adalah solusi ideal untuk memigrasi, mencadangkan, atau mem-burst aplikasi berbasis file Anda dari lokal ke lokasi AWS tanpa perlu mengubah kode aplikasi atau cara Anda mengelola data.

Sebagai layanan yang dikelola sepenuhnya, FSx untuk ONTAP memudahkan peluncuran dan skala penyimpanan file bersama yang andal, berkinerja tinggi, dan aman di cloud. Dengan fsX untuk ONTAP, Anda tidak perlu lagi khawatir tentang:

- Menyiapkan dan menyediakan server file dan volume penyimpanan
- Mereplikasi data
- Menginstal dan menambal perangkat lunak server file
- Mendeteksi dan mengatasi kegagalan perangkat keras

- Mengelola failover dan failback
- Melakukan backup secara manual

FSx untuk ONTAP juga menyediakan integrasi yang kaya dengan AWS layanan lain, seperti AWS Identity and Access Management (IAM), Amazon, AWS Key Management Service (AWS KMS) WorkSpaces, dan. AWS CloudTrail

Topik

- Fitur FSx untuk ONTAP
- Keamanan dan perlindungan data
- Harga untuk FSx untuk ONTAP
- fsX untuk forum ONTAP
- Apakah Anda pengguna Amazon FSx pertama kali?

Fitur FSx untuk ONTAP

Dengan fsX untuk ONTAP, Anda mendapatkan solusi penyimpanan file yang dikelola sepenuhnya dengan:

- Support untuk dataset skala petabyte dalam satu namespace
- Hingga puluhan gigabyte per detik (GBps) throughput per sistem file
- Akses multi-protokol ke data menggunakan protokol Network File System (NFS), Server Message Block (SMB), dan Internet Small Computer Systems Interface (iSCSI)
- Opsi penyebaran Multi-AZ dan Single-AZ yang sangat tersedia dan tahan lama
- Tingkat data otomatis yang mengurangi biaya penyimpanan dengan secara otomatis mentransisikan data yang jarang diakses ke tingkat penyimpanan berbiaya lebih rendah berdasarkan pola akses Anda
- Kompresi data, deduplikasi, dan pemadatan untuk mengurangi konsumsi penyimpanan Anda
- Dukungan untuk NetApp fitur SnapMirror replikasi
- Support untuk NetApp solusi caching lokal: NetApp Global File Cache dan FlexCache
- Support untuk akses dan manajemen menggunakan native AWS atau NetApp tools dan operasi API
  - AWS Management Console, AWS Command Line Interface (AWS CLI), dan SDK

  - NetApp ONTAP CLI, REST API, dan BlueXP
- Support untuk fitur perlindungan dan keamanan data berikut:
  - Enkripsi data sistem file dan backup saat istirahat menggunakan AWS KMS keys
  - Enkripsi data dalam perjalanan menggunakan kunci sesi SMB Kerberos
  - Pemindaian antivirus sesuai permintaan
  - Otentikasi dan otorisasi menggunakan Microsoft Active Directory
  - Mengaudit akses kunci
  - NetAppSnapLockFitur WORM dengan dukungan untuk Volume Kepatuhan dan Perusahaan

Keamanan dan perlindungan data

Amazon FSx menyediakan berbagai tingkat keamanan dan kepatuhan untuk memfasilitasi perlindungan data Anda. Ini secara otomatis mengenkripsi data saat istirahat dalam sistem file dan backup menggunakan kunci yang Anda kelola di (). AWS Key Management Service AWS KMS Anda juga dapat mengenkripsi data dalam perjalanan menggunakan Kerberos untuk klien NFS dan SMB.

Amazon FSx telah dinilai untuk mematuhi standar berikut:

- Organisasi Standar Internasional (ISO)
- Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS)
- Sertifikasi Sistem dan Kontrol Organisasi (SOC)
- Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan 1996 (HIPAA)

Untuk informasi selengkapnya, lihat Perlindungan data di Amazon FSx untuk ONTAP NetApp .

Amazon FSx juga menyediakan tingkat kontrol akses berikut:

- Pada tingkat sistem file, Amazon FSx menyediakan kontrol akses dengan menggunakan grup keamanan Amazon Virtual Private Cloud (Amazon VPC).
- Pada tingkat API, Amazon FSx menyediakan kontrol akses dengan menggunakan kebijakan akses AWS Identity and Access Management (IAM).
- Untuk menyediakan kontrol akses pada tingkat file dan folder, Amazon FSx mendukung izin Unix, daftar kontrol akses NFS (ACL), dan NTFS ACL. Saat Anda bergabung dengan Amazon FSx ke Active Directory, pengguna yang mengakses sistem file dapat mengautentikasi menggunakan kredensyal Direktori Aktif mereka.

Agar Anda dapat melihat tindakan yang diambil oleh pengguna di sumber daya Amazon FSx Anda, Amazon FSx terintegrasi dengan AWS CloudTrail untuk memantau dan mencatat panggilan API Amazon FSx Anda. Untuk informasi selengkapnya, lihat Logging FSx untuk Panggilan API ONTAP denganAWS CloudTrail.

Selain itu, Amazon FSx melindungi data Anda dengan cadangan sistem file yang sangat tahan lama. Amazon FSx melakukan pencadangan harian otomatis, dan Anda dapat mengambil cadangan tambahan kapan saja. Untuk informasi selengkapnya, lihat Melindungi data Anda.

Harga untuk FSx untuk ONTAP

Anda ditagih untuk sistem file berdasarkan kategori berikut:

- Kapasitas penyimpanan SSD (per gigabyte-bulan, atau GB-bulan)
- SSD IOPS yang Anda berikan di atas tiga IOPS/GB (per IOP-bulan)
- Kapasitas throughput (per megabyte per detik [MBps] -bulan)
- Konsumsi penyimpanan kolam kapasitas (per GB-bulan)
- Permintaan kolam kapasitas (per baca dan tulis)
- Konsumsi penyimpanan cadangan (per GB-bulan)

Untuk informasi selengkapnya tentang harga dan biaya yang terkait dengan layanan, lihat Amazon FSx untuk harga NetApp ONTAP.

fsX untuk forum ONTAP

Jika Anda mengalami masalah saat menggunakan Amazon FSx, gunakan forum diskusi fsX untuk ONTAP untuk mendapatkan jawaban.

Apakah Anda pengguna Amazon FSx pertama kali?

Jika Anda adalah pengguna pertama kali Amazon FSx, kami sarankan Anda membaca bagian berikut secara berurutan:

1. Jika Anda baru mengenal AWS, lihat Menyiapkan fsX untuk ONTAP untuk menyiapkan Akun AWS.

2. Jika Anda siap membuat sistem file Amazon FSx pertama Anda, ikuti petunjuknya. Memulai Amazon FSx untuk ONTAP NetApp
3. Untuk informasi tentang kinerja, lihatAmazon FSx untuk NetApp kinerja ONTAP.
4. Untuk detail keamanan Amazon FSx, lihat Keamanan di Amazon FSx untuk ONTAP NetApp .
5. Untuk informasi tentang Amazon FSx API, lihat Referensi API Amazon FSx.

Cara kerja Amazon FSx untuk NetApp ONTAP

Topik ini memperkenalkan fitur utama Amazon FSx NetApp untuk sistem file ONTAP dan cara kerjanya, dengan tautan ke bagian dengan deskripsi mendalam, detail implementasi penting, dan prosedur konfigurasi. step-by-step

Topik

fsX untuk sistem file ONTAP

Sistem file adalah FSx utama untuk sumber daya ONTAP, analog dengan kluster ONTAP lokal. NetApp Anda menentukan kapasitas penyimpanan solid state drive (SSD) dan kapasitas throughput untuk sistem file Anda, dan pilih Amazon Virtual Private Cloud (VPC) tempat sistem file Anda dibuat. Untuk informasi selengkapnya, lihat Mengelola fsX untuk sistem file ONTAP.

Sistem file Anda dapat memiliki satu hingga 12 pasangan ketersediaan tinggi (HA) tergantung pada konfigurasinya. Pasangan HA terdiri dari dua server file dalam konfigurasi siaga aktif. Sistem file dengan pasangan HA tunggal disebut sistem file scale-up. Sistem file dengan beberapa pasangan HA disebut sistem file scale-out. Untuk informasi selengkapnya, lihat Pasangan ketersediaan tinggi (HA).

Penyimpanan mesin virtual

Storage Virtual Machine (SVM) adalah file server terisolasi dengan endpoint administratif dan akses data sendiri untuk mengelola dan mengakses data. Saat Anda mengakses data di FSx untuk sistem file ONTAP, klien dan workstation Anda berinteraksi dengan SVM menggunakan alamat IP titik akhir SVM. Untuk informasi selengkapnya, lihat Mengelola SVM.

Anda dapat menggabungkan SVM ke Microsoft Active Directory untuk otentikasi dan otorisasi akses file. Untuk informasi selengkapnya, lihat Bekerja dengan Microsoft Active Directory di FSx untuk ONTAP.

Volume

FSx untuk volume ONTAP adalah sumber daya virtual yang Anda gunakan untuk mengatur dan mengelompokkan data Anda. Volume adalah wadah logis yang di-host di SVM, dan data yang disimpan di dalamnya menghabiskan kapasitas penyimpanan fisik pada sistem file Anda.

Saat Anda membuat volume, Anda mengatur ukurannya, yang menentukan jumlah data fisik yang dapat Anda simpan di dalamnya, terlepas dari tingkat penyimpanan mana data disimpan. Anda juga mengatur jenis volume, baik RW (read-writable) atau DP (perlindungan data). Volume DP adalah read-only dan dapat digunakan sebagai tujuan dalam hubungan atau NetApp SnapMirror . SnapVault

FSx untuk volume ONTAP disediakan tipis, artinya mereka hanya mengkonsumsi kapasitas penyimpanan untuk data yang tersimpan di dalamnya. Dengan volume yang disediakan tipis, kapasitas penyimpanan tidak dicadangkan terlebih dahulu. Sebaliknya, penyimpanan dialokasikan secara dinamis, seperti yang diperlukan. Ruang kosong dilepaskan kembali ke sistem file ketika data dalam volume atau LUN dihapus. Misalnya, Anda dapat membuat tiga volume 10 TiB pada sistem file yang dikonfigurasi dengan kapasitas penyimpanan gratis 10 TiB, selama jumlah total data yang disimpan dalam tiga volume tidak melebihi 10 TiB setiap saat. Jumlah data yang disimpan secara fisik pada volume dihitung terhadap konsumsi kapasitas penyimpanan Anda secara keseluruhan. Untuk informasi selengkapnya, lihat Mengelola FSx untuk volume ONTAP.

Tingkatan penyimpanan

Sistem file FSx untuk ONTAP memiliki dua tingkatan penyimpanan: penyimpanan primer dan penyimpanan kolam kapasitas. Penyimpanan primer disediakan, dapat diskalakan, penyimpanan SSD berkinerja tinggi yang dibuat khusus untuk bagian aktif kumpulan data Anda. Penyimpanan kolam kapasitas adalah tingkat penyimpanan yang sepenuhnya elastis yang dapat menskalakan hingga ukuran petabyte dan dioptimalkan biaya untuk data yang jarang diakses. Data yang Anda tulis ke volume Anda menghabiskan kapasitas pada tingkatan penyimpanan Anda. Untuk informasi selengkapnya, lihat fsX untuk tingkatan penyimpanan ONTAP.

Tingkatan data

Tingkatan data adalah proses dimana Amazon FSx NetApp untuk ONTAP secara otomatis memindahkan data antara SSD dan tingkatan penyimpanan kumpulan kapasitas. Setiap volume memiliki kebijakan tiering yang mengontrol apakah data dipindahkan ke tingkat kapasitas ketika menjadi tidak aktif (dingin). Periode pendinginan kebijakan Tiering volume menentukan kapan data menjadi tidak aktif (dingin). Untuk informasi selengkapnya, lihat Tingkat data volume.

Efisiensi penyimpanan

Amazon FSx untuk NetApp ONTAP mendukung fitur efisiensi penyimpanan tingkat blok ONTAP —pemadatan, kompresi, dan deduplikasi — untuk mengurangi kapasitas penyimpanan yang dikonsumsi data Anda. Fitur efisiensi penyimpanan dapat mengurangi jejak data Anda dalam penyimpanan SSD, penyimpanan kolam kapasitas, dan cadangan. Penghematan kapasitas penyimpanan tipikal untuk beban kerja berbagi file tujuan umum tanpa mengorbankan kinerja adalah 65% dari kompresi, deduplikasi, dan pemadatan, baik pada SSD maupun tingkatan penyimpanan kolam kapasitas. Untuk informasi selengkapnya, lihat fsX untuk efisiensi penyimpanan ONTAP.

Mengakses data yang disimpan di FSx untuk sistem file ONTAP

Anda dapat mengakses data Anda di FSx untuk volume ONTAP dari beberapa klien Linux, Windows, atau macOS secara bersamaan melalui protokol NFS (v3, v4, v4.1, v4.2) dan SMB. Anda juga dapat mengakses data menggunakan protokol iSCSI (blok). Untuk informasi selengkapnya, lihat Mengakses data.

Mengelola FSx untuk sumber daya ONTAP

Ada beberapa cara agar Anda dapat berinteraksi dengan FSx Anda untuk sistem file ONTAP dan mengelola sumber dayanya. Anda dapat mengelola FSx Anda untuk sumber daya ONTAP menggunakan keduanya AWS dan alat manajemen NetApp ONTAP:

- AWS alat manajemen
  - The AWS Management Console
  - AWS Command Line Interface (AWS CLI)
  - Amazon FSx API dan SDK
  - AWS CloudFormation

- NetApp alat manajemen:
  - NetApp BlueXP
  - CLI NetApp ONTAP
  - API REST NetApp ONTAP

Untuk informasi selengkapnya, lihat Mengelola sumber daya.

Menyiapkan fsX untuk ONTAP

Sebelum Anda menggunakan Amazon FSx untuk pertama kali, selesaikan tugas berikut:

1. Mendaftar untuk Akun AWS
2. Buat pengguna dengan akses administratif

Topik

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/signup.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan mengunjungi https://aws.amazon.com/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

   Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.

2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .

2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.
2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Langkah selanjutnya

Untuk mulai menggunakan FSx untuk ONTAP, lihat petunjuk Memulai Amazon FSx untuk ONTAP NetApp untuk membuat sumber daya Amazon FSx Anda.

Memulai Amazon FSx untuk ONTAP NetApp

Pelajari cara memulai menggunakan Amazon FSx untuk NetApp ONTAP. Latihan memulai ini mencakup langkah-langkah berikut.

Topik

Langkah 1: Buat Amazon FSx untuk sistem file NetApp ONTAP

Konsol Amazon FSx memiliki dua opsi untuk membuat sistem file - opsi Buat cepat dan opsi buat Standar. Untuk membuat Amazon fsX untuk sistem file NetApp ONTAP dengan cepat dan mudah dengan konfigurasi yang direkomendasikan layanan, gunakan opsi Buat cepat.

Opsi Quick create menciptakan sistem file dengan single high-availability pair (HA), single storage virtual machine (SVM) dan satu volume. Opsi Quick create mengkonfigurasi sistem file ini untuk memungkinkan akses data dari instance Linux melalui protokol Network File System (NFS). Setelah sistem file dibuat, Anda dapat membuat SVM dan volume tambahan sesuai kebutuhan, termasuk SVM yang digabungkan ke Active Directory untuk memungkinkan akses dari klien Windows dan macOS melalui protokol Server Message Block (SMB).

Untuk informasi tentang menggunakan opsi Buat Standar untuk membuat sistem file dengan konfigurasi yang disesuaikan, dan untuk menggunakan API AWS CLI dan, lihatMembuat fsX untuk sistem file ONTAP.

Untuk membuat sistem file Anda

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Pada dasbor, pilih Buat sistem file untuk memulai wizard pembuatan sistem file.
3. Pada halaman Pilih jenis sistem file, pilih Amazon FSx untuk NetApp ONTAP, lalu pilih Berikutnya. Halaman Create ONTAP file system muncul.
4. Untuk metode Creation, pilih Quick create.
5. Di bagian Konfigurasi cepat, untuk Nama sistem file - opsional, masukkan nama untuk sistem file Anda. Lebih mudah untuk menemukan dan mengelola sistem file Anda ketika Anda

menamainya. Anda dapat menggunakan maksimal 256 huruf Unicode, spasi putih, dan angka, ditambah karakter khusus ini: + - (tanda hubung) =. _ (garis bawah):/

6. Untuk Jenis Deployment Pilih Multi-AZ atau Single-AZ.

   - Sistem file multi-AZ mereplikasi data Anda dan mendukung failover di beberapa Availability Zone secara bersamaan. Wilayah AWS
   - Sistem file single-AZ mereplikasi data Anda dan menawarkan failover otomatis dalam satu Availability Zone.

   Untuk informasi selengkapnya, lihat Ketersediaan dan daya tahan.

7. Untuk kapasitas penyimpanan SSD, tentukan kapasitas penyimpanan sistem file Anda, dalam gibibytes (GiB). Masukkan bilangan bulat apa pun dalam kisaran 1.024—196.608. Jika Anda membutuhkan lebih banyak kapasitas penyimpanan SSD, Anda dapat menggunakan Standard create. Untuk informasi selengkapnya, lihat Untuk membuat sistem file (konsol).

   Anda dapat meningkatkan jumlah kapasitas penyimpanan sesuai kebutuhan setiap saat setelah Anda membuat sistem file. Untuk informasi selengkapnya, lihat Mengelola kapasitas penyimpanan.

8. Untuk kapasitas Throughput, Amazon FSx secara otomatis menyediakan kapasitas throughput yang direkomendasikan berdasarkan penyimpanan SSD Anda. Anda juga dapat memilih throughput sistem file Anda (hingga 4.096 MBps). Jika Anda membutuhkan lebih banyak kapasitas throughput, Anda dapat menggunakan Standard create.
9. Untuk Virtual Private Cloud (VPC), pilih Amazon VPC yang ingin Anda kaitkan dengan sistem file Anda.
10. Untuk efisiensi Penyimpanan, pilih Diaktifkan untuk mengaktifkan fitur efisiensi penyimpanan ONTAP (kompresi, deduplikasi, dan pemadatan) atau Dinonaktifkan untuk mematikannya.
11. (Hanya multi-AZ) Rentang alamat IP titik akhir menentukan rentang alamat IP di mana titik akhir untuk mengakses sistem file Anda dibuat.

    Pilih opsi Buat cepat untuk rentang alamat IP titik akhir:

    - Rentang alamat IP yang tidak dialokasikan dari VPC Anda - Pilih opsi ini agar Amazon FSx menggunakan 64 alamat IP terakhir dari rentang CIDR utama VPC sebagai rentang alamat IP titik akhir untuk sistem file. Perhatikan bahwa rentang ini dibagi di beberapa sistem file jika Anda memilih opsi ini beberapa kali.

> **Note**
>
> - Setiap sistem file yang Anda buat menggunakan dua alamat IP dari rentang ini—satu untuk cluster, dan satu untuk SVM pertama. Alamat IP pertama dan terakhir juga dicadangkan. Untuk setiap SVM tambahan, sistem file mengkonsumsi alamat IP lain. Misalnya, sistem file yang menampung 10 SVM menggunakan 11 alamat IP. Sistem file tambahan bekerja dengan cara yang sama. Mereka menggunakan dua alamat IP awal, ditambah satu untuk setiap SVM tambahan. Jumlah maksimum sistem file yang menggunakan rentang alamat IP yang sama, masing-masing dengan SVM tunggal, adalah 31.
> - Opsi ini berwarna abu-abu jika salah satu dari 64 alamat IP terakhir dalam rentang CIDR utama VPC digunakan oleh subnet.

- Rentang alamat IP mengambang di luar VPC Anda - Pilih opsi ini agar Amazon FSx menggunakan rentang alamat 198.19.x.0/24 yang belum digunakan oleh sistem file lain dengan VPC dan tabel rute yang sama.

Anda juga dapat menentukan rentang alamat IP Anda sendiri di opsi Buat standar.

12. Pilih Berikutnya, dan tinjau konfigurasi sistem file pada halaman Create ONTAP file system. Perhatikan pengaturan sistem file mana yang dapat Anda modifikasi setelah sistem file dibuat.
13. Pilih Buat sistem file.

Quick create membuat sistem file dengan satu SVM (bernama`fsx`) dan satu volume (bernama`vol1`). Volume memiliki jalur persimpangan `/vol1` dan kebijakan tingkatan kumpulan kapasitas Auto (yang secara otomatis akan memberi peringkat data apa pun yang belum diakses selama 31 hari ke penyimpanan kolam berkapasitas lebih rendah). Kebijakan snapshot default ditetapkan ke volume default. Data sistem file dienkripsi saat istirahat menggunakan kunci terkelola AWS KMS layanan default Anda.

Langkah 2: Memasang sistem file Anda dari instans Amazon EC2 Linux

Anda dapat memasang sistem file dari instans Amazon Elastic Compute Cloud (Amazon EC2). Prosedur ini menggunakan instance yang menjalankan Amazon Linux 2.

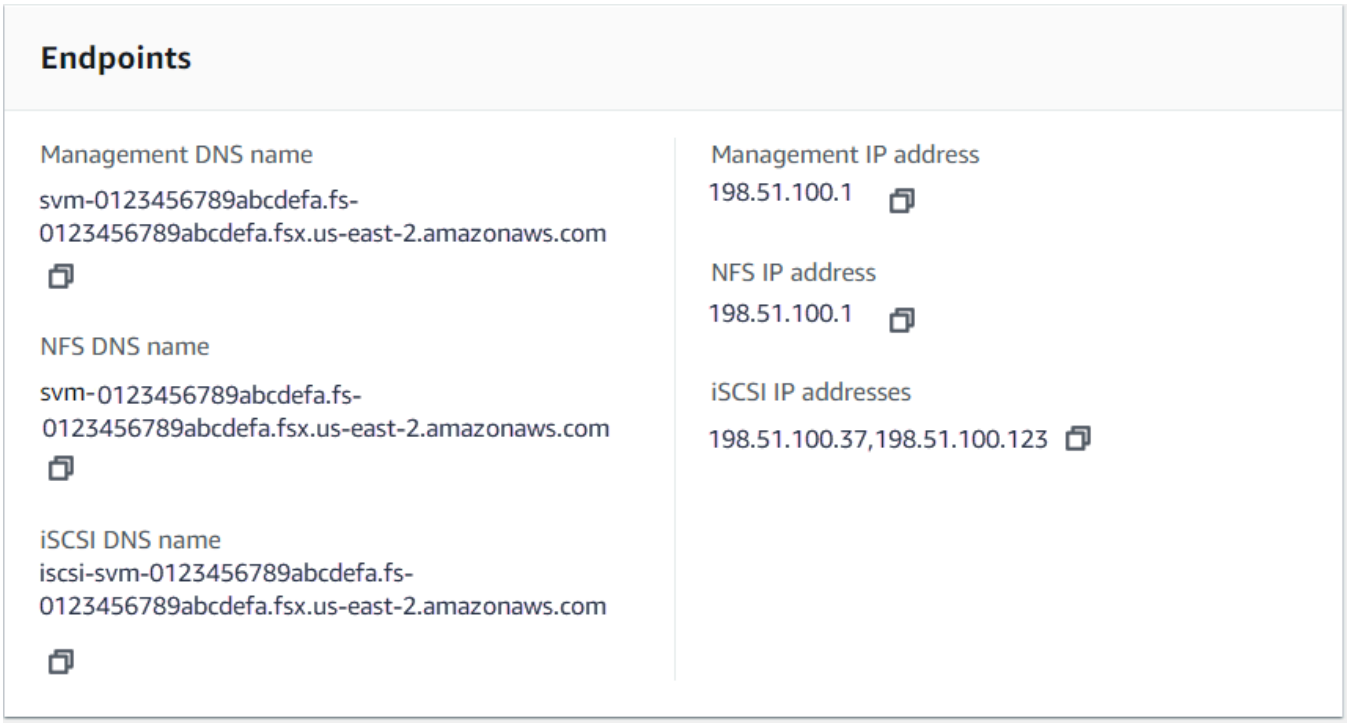
Untuk memasang sistem file Anda dari Amazon EC2

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Buat atau pilih instans Amazon EC2 yang menjalankan Amazon Linux 2 yang berada di cloud pribadi virtual (VPC) yang sama dengan sistem file Anda. Untuk informasi selengkapnya tentang meluncurkan instans, lihat Langkah 1: Meluncurkan instans di Panduan Pengguna Amazon EC2.
3. Connect ke instans Amazon EC2 Linux Anda. Untuk informasi selengkapnya, lihat Connect ke instans Linux Anda di Panduan Pengguna Amazon EC2.
4. Buka terminal di instans Amazon EC2 Anda menggunakan shell aman (SSH), dan masuk dengan kredensi yang sesuai.
5. Buat direktori di instans Amazon EC2 Anda untuk digunakan sebagai titik pemasangan volume dengan perintah berikut. Dalam contoh berikut, ganti *mount point dengan informasi* Anda sendiri.

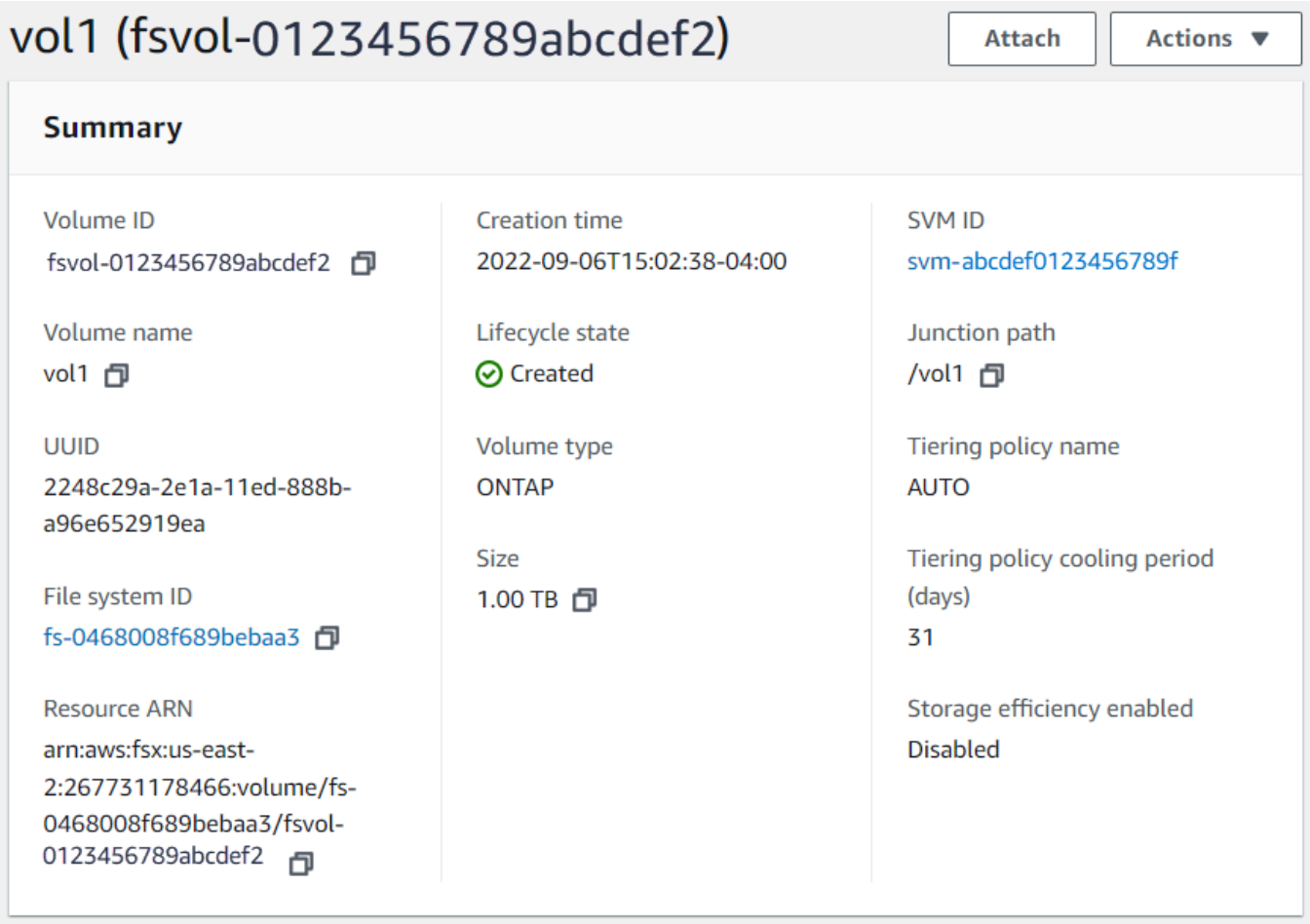
   ```
   $ sudo mkdir /mount-point
   ```

6. Pasang Amazon FSx Anda untuk sistem file NetApp ONTAP ke direktori yang Anda buat. Gunakan `mount` perintah yang mirip dengan contoh berikut. Dalam contoh berikut, ganti nilai placeholder berikut dengan informasi Anda sendiri.

   - *nfs_version*— Versi NFS yang Anda gunakan; FSx untuk ONTAP mendukung versi 3, 4.0, 4.1, dan 4.2.
   - *nfs-dns-name*— Nama DNS NFS dari mesin virtual penyimpanan (SVM) di mana volume yang Anda pasang ada. Anda dapat menemukan nama DNS NFS di konsol Amazon FSx dengan memilih mesin virtual Penyimpanan, lalu memilih SVM tempat volume yang Anda pasang ada. Nama DNS NFS ditemukan pada panel Endpoints, yang ditunjukkan pada gambar berikut.



- *`volume-junction-path`*— Jalur persimpangan volume yang Anda pasang. Anda dapat menemukan jalur persimpangan volume di konsol Amazon FSx pada panel Ringkasan halaman Detail volume, yang ditunjukkan pada gambar berikut.



- *mount-point*— Nama direktori yang Anda buat pada instans EC2 Anda untuk titik pemasangan volume.

```
sudo mount -t nfs -o nfsvers=nfs_version nfs-dns-name:/volume-junction-path /mount-point
```

Perintah berikut menggunakan nilai contoh.

```
sudo mount -t nfs -o nfsvers=4.1 svm-abcdef1234567890c.fs-012345abcdef6789b.fsx.us-east-2.amazonaws.com:/vol1 /fsxN
```

Jika Anda memiliki masalah dengan instans Amazon EC2 (seperti waktu habis koneksi), lihat Memecahkan masalah instans EC2 di Panduan Pengguna Amazon EC2.

Langkah 3: Bersihkan Sumber Daya

Setelah Anda menyelesaikan latihan ini, Anda harus mengikuti langkah-langkah ini untuk membersihkan sumber daya Anda dan melindungi Anda Akun AWS.

Untuk membersihkan sumber daya

1. Pada konsol Amazon EC2, akhiri instans Anda. Untuk informasi selengkapnya, lihat Menghentikan Instans Anda di Panduan Pengguna Amazon EC2.
2. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
3. Di konsol Amazon FSx, hapus semua FSx Anda untuk volume ONTAP yang bukan volume root SVM Anda. Untuk informasi selengkapnya, lihat Menghapus volume.
4. Hapus semua FSx Anda untuk ONTAP SVM. Untuk informasi selengkapnya, lihat Menghapus penyimpanan virtual machine (SVM).
5. Pada konsol Amazon FSx, hapus sistem file Anda. Ketika Anda menghapus sistem file, semua backup otomatis dihapus secara otomatis. Namun, Anda masih harus menghapus cadangan yang dibuat secara manual. Langkah-langkah berikut menguraikan proses ini.

    a. Dari dasbor konsol, pilih nama sistem file yang Anda buat untuk latihan ini.

    b. Untuk Tindakan, pilih Hapus sistem file.

    c. Dalam kotak dialog Hapus sistem file, masukkan ID sistem file yang ingin Anda hapus di kotak ID sistem file.

    d. Pilih Hapus sistem file.

    e. Sementara Amazon FSx menghapus sistem file, statusnya di dasbor berubah menjadi DELETING. Setelah sistem file dihapus, itu tidak lagi muncul di dasbor. Setiap backup otomatis dihapus bersama dengan sistem file.

    f. Sekarang Anda dapat menghapus backup apa pun yang dibuat secara manual untuk sistem file Anda. Dari navigasi sisi kiri, pilih Backup.

    g. Dari dasbor, pilih backup apa pun yang memiliki ID sistem file yang sama dengan sistem file yang Anda hapus, dan pilih Hapus backup. Pastikan untuk menyimpan cadangan akhir, jika Anda membuatnya.

    h. Kotak dialog Hapus backup terbuka. Simpan kotak centang yang dipilih untuk ID cadangan yang ingin Anda hapus, lalu pilih Hapus cadangan.

Sistem file Amazon FSx Anda dan cadangan otomatis terkait sekarang dihapus, bersama dengan cadangan manual apa pun yang Anda pilih untuk dihapus juga.

Mengakses data

Anda dapat mengakses sistem file Amazon FSx Anda menggunakan berbagai klien dan metode yang didukung baik di lingkungan AWS Cloud maupun di tempat.

Setiap SVM memiliki empat titik akhir yang digunakan untuk mengakses data atau mengelola SVM menggunakan ONTAP NetApp CLI atau REST API:

- `Nfs`— Untuk menghubungkan menggunakan protokol Network File System (NFS)
- `Smb`— Untuk menghubungkan menggunakan protokol Service Message Block (SMB) (Jika SVM Anda bergabung ke Active Directory, atau Anda menggunakan workgroup.)
- `Iscsi`— Untuk menghubungkan menggunakan protokol Internet Small Computer Systems Interface (iSCSI) (hanya untuk sistem file scale-up).
- `Management`— Untuk mengelola SVM menggunakan NetApp ONTAP CLI atau API, atau BlueXP NetApp

Topik

Klien yang didukung

FSx untuk sistem file ONTAP mendukung akses data dari berbagai contoh komputasi dan sistem operasi. Ini dilakukan dengan mendukung akses menggunakan protokol Network File System (NFS) (v3, v4.0, v4.1 dan v4.2), semua versi protokol Server Message Block (SMB) (termasuk 2.0, 3.0, dan 3.1.1), dan protokol Internet Small Computer Systems Interface (iSCSI).

> **Important**
>
> Amazon FSx tidak support akses sistem file dari internet publik. Amazon FSx secara otomatis melepaskan alamat IP Elastic yang merupakan alamat IP publik yang dapat dijangkau dari Internet, yang dilampirkan ke antarmuka network elastis sistem file.

Instans AWS komputasi berikut didukung untuk digunakan dengan fsX untuk ONTAP:

- Instans Amazon Elastic Compute Cloud (Amazon EC2) menjalankan Linux dengan dukungan NFS atau SMB, Microsoft Windows, dan macOS. Untuk informasi selengkapnya, lihat Volume pemasangan.
- Amazon Elastic Container Service (Amazon ECS) Container Docker di instans Amazon EC2 Windows dan Linux. Untuk informasi selengkapnya, lihat Menggunakan Amazon Elastic Container Service dengan FSx untuk ONTAP.
- Amazon Elastic Kubernetes Service — Untuk mempelajari selengkapnya, lihat Amazon fsX untuk driver NetApp ONTAP CSI di Panduan Pengguna Amazon EKS.
- Red Hat OpenShift Service on AWS (ROSA) — Untuk mempelajari lebih lanjut, lihat Apa itu OpenShift Layanan Red Hat? AWS dalam OpenShift Layanan Red Hat pada Panduan AWS Pengguna.
- WorkSpaces Contoh Amazon. Untuk informasi selengkapnya, lihat Menggunakan Amazon WorkSpaces dengan FSx untuk ONTAP.
- Instans Amazon AppStream 2.0.
- AWS Lambda — Untuk informasi lebih lanjut, lihat posting AWS blog Mengaktifkan akses SMB untuk beban kerja tanpa server dengan Amazon FSx.
- Mesin virtual (VM) berjalan di VMware Cloud di lingkungan. AWS Untuk informasi selengkapnya, lihat Mengonfigurasi Amazon FSx untuk NetApp ONTAP sebagai Penyimpanan Eksternal dan VMware Cloud dengan AWS Amazon FSx untuk Panduan Penerapan ONTAP. NetApp

Setelah dipasang, fsX untuk sistem file ONTAP muncul sebagai direktori lokal atau huruf drive melalui NFS dan SMB, menyediakan penyimpanan file jaringan bersama yang dikelola sepenuhnya yang dapat diakses secara bersamaan oleh hingga ribuan klien. iSCSI LUNS dapat diakses sebagai perangkat blok saat dipasang melalui iSCSI.

Mengakses data dari dalam AWS

Setiap sistem file Amazon FSx dikaitkan dengan Virtual Private Cloud (VPC). Anda dapat mengakses FSx Anda untuk sistem file ONTAP dari mana saja di VPC sistem file, terlepas dari Availability Zone. Anda juga dapat mengakses sistem file Anda dari VPC lain yang dapat berada di AWS akun yang berbeda atau Wilayah AWS. Selain persyaratan yang dijelaskan di bagian berikut untuk mengakses FSx untuk sumber daya ONTAP, Anda juga perlu memastikan bahwa grup keamanan VPC sistem file Anda dikonfigurasi sehingga lalu lintas data dan manajemen dapat mengalir antara sistem file dan klien Anda. Untuk informasi selengkapnya tentang mengonfigurasi grup keamanan dengan port yang diperlukan, lihatGrup keamanan Amazon VPC.

Topik

- Mengakses data dari dalam VPC yang sama
- Mengakses data dari luar VPC penyebaran

Mengakses data dari dalam VPC yang sama

Saat Anda membuat Amazon FSx untuk sistem file NetApp ONTAP, Anda memilih Amazon VPC di mana ia berada. Semua SVM dan volume yang terkait dengan Amazon FSx NetApp untuk sistem file ONTAP juga terletak di VPC yang sama. Saat memasang volume, jika sistem file dan klien yang memasang volume terletak di VPC yang sama dan Akun AWS, Anda dapat menggunakan nama DNS SVM dan sambungan volume atau berbagi SMB, tergantung pada klien. Untuk informasi selengkapnya, lihat Volume pemasangan.

Anda dapat mencapai kinerja optimal jika klien dan volume berada di Availability Zone yang sama dengan subnet sistem file, atau subnet pilihan untuk sistem file multi-AZ. Untuk mengidentifikasi subnet sistem file atau subnet pilihan, di konsol Amazon FSx, pilih sistem File, lalu pilih sistem file ONTAP yang volumenya Anda pasang, dan subnet atau subnet pilihan (Multi-AZ) ditampilkan di Subnet atau Preferred subnet panel.

Mengakses data dari luar VPC penyebaran

Bagian ini menjelaskan cara mengakses FSx untuk titik akhir sistem file ONTAP dari AWS lokasi di luar VPC penyebaran sistem file.

Mengakses titik akhir manajemen NFS, SMB, dan ONTAP pada sistem file multi-AZ

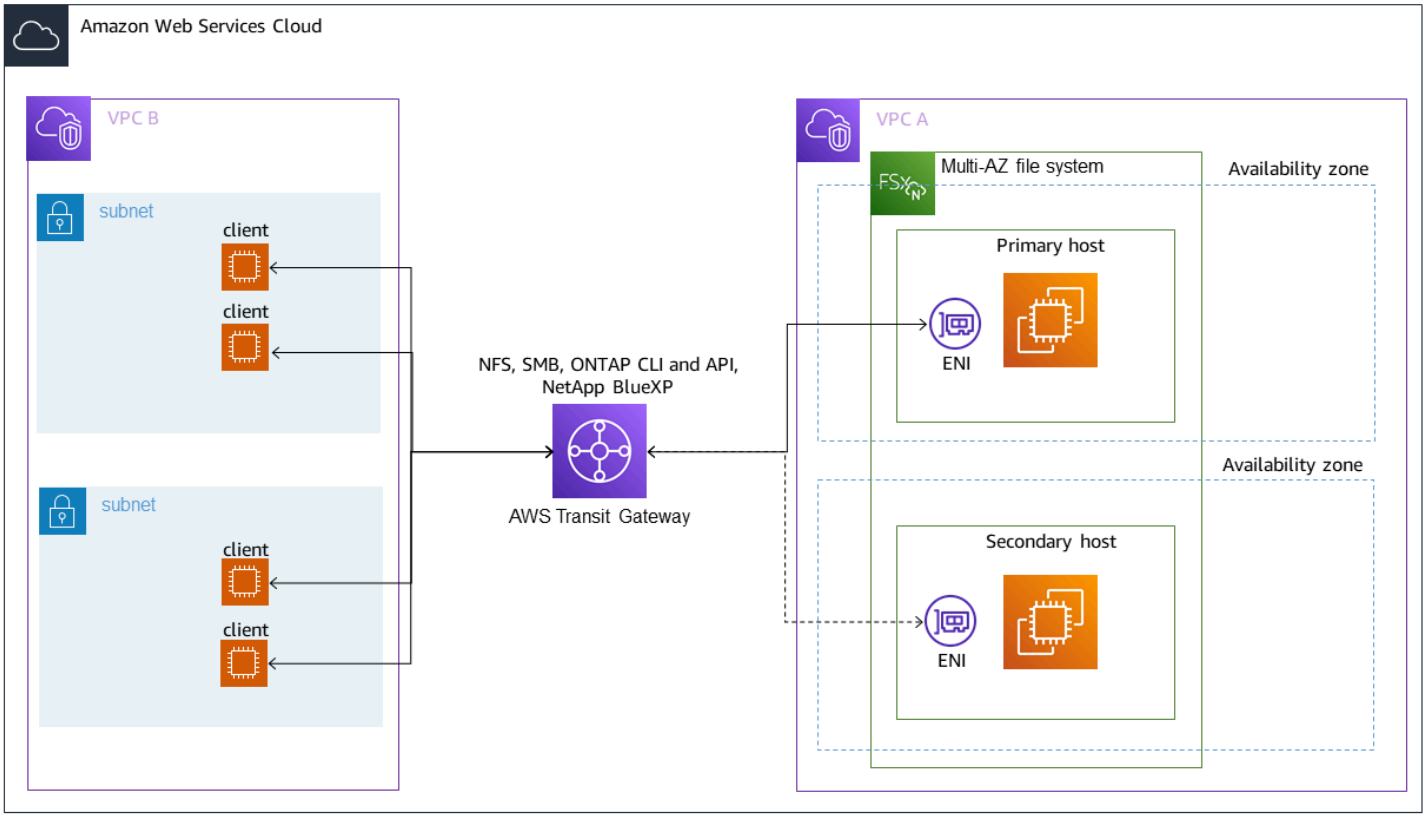
Titik akhir manajemen NFS, SMB, dan ONTAP di Amazon FSx NetApp untuk sistem file Multi-AZ ONTAP menggunakan alamat protokol internet mengambang (IP) sehingga klien yang terhubung dengan mulus bertransisi antara server file pilihan dan siaga selama acara failover. Untuk informasi selengkapnya tentang failover, lihat Proses failover untuk FSx untuk ONTAP.

Alamat IP mengambang ini dibuat dalam tabel rute VPC yang Anda kaitkan dengan sistem file Anda, dan berada dalam sistem file `EndpointIpAddressRange` yang dapat Anda tentukan selama pembuatan. `EndpointIpAddressRange`Menggunakan rentang alamat berikut, tergantung pada bagaimana sistem file dibuat:

- Sistem file multi-AZ yang dibuat menggunakan konsol Amazon FSx menggunakan 64 alamat IP terakhir dalam rentang CIDR utama VPC untuk sistem file secara default. `EndpointIpAddressRange`
- Sistem file multi-AZ yang dibuat menggunakan AWS CLI atau Amazon FSx API menggunakan rentang alamat IP dalam `198.19.0.0/16` blok alamat untuk `EndpointIpAddressRange` secara default.

Hanya AWS Transit Gatewaymendukung routing ke alamat IP mengambang, yang juga dikenal sebagai transitive peering. VPC Peering, AWS Direct Connect, dan AWS VPN tidak mendukung pengintip transitif. Oleh karena itu, Anda diharuskan menggunakan Transit Gateway untuk mengakses antarmuka ini dari jaringan yang berada di luar VPC sistem file Anda.

Diagram berikut menggambarkan penggunaan Transit Gateway untuk NFS, SMB, atau akses manajemen ke sistem file Multi-AZ yang berada di VPC yang berbeda dari klien yang mengaksesnya.



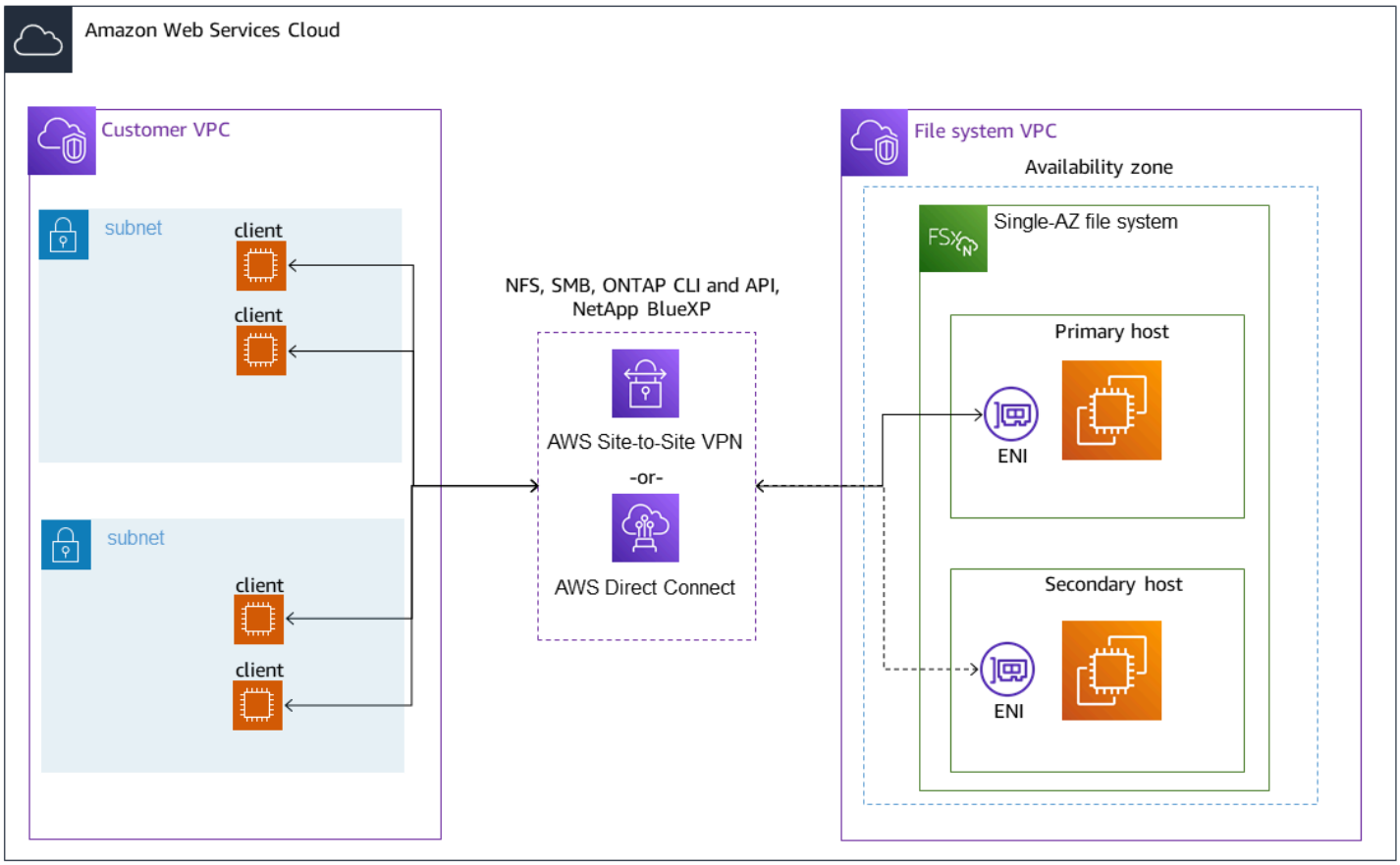
> **Note**
>
> Pastikan bahwa semua tabel rute yang Anda gunakan terkait dengan sistem file Multi-AZ Anda. Melakukannya membantu mencegah tidak tersedianya selama failover. Untuk informasi tentang mengaitkan tabel rute VPC Amazon Anda dengan sistem file Anda, lihat. Memperbarui sistem file

Untuk informasi tentang kapan Anda perlu menggunakan Transit Gateway untuk mengakses fsX Anda untuk sistem file ONTAP, lihat. Kapan Transit Gateway diperlukan?

Mengakses NFS, SMB, atau ONTAP CLI dan API untuk sistem file single-AZ

Titik akhir yang digunakan untuk mengakses FSx untuk sistem file ONTAP Single-AZ melalui NFS atau SMB, dan untuk mengelola sistem file menggunakan ONTAP CLI atau REST API, adalah alamat IP sekunder pada ENI dari server file aktif. Alamat IP sekunder berada dalam rentang CIDR VPC, sehingga klien dapat mengakses data dan port manajemen menggunakan VPC Peering,, atau tanpa memerlukan. AWS Direct Connect AWS VPN AWS Transit Gateway

Diagram berikut menggambarkan penggunaan AWS VPN atau AWS Direct Connect untuk NFS, SMB, atau akses manajemen ke sistem file Single-AZ yang berada di VPC yang berbeda dari klien yang mengaksesnya.



Kapan Transit Gateway diperlukan?

Apakah Transit Gateway diperlukan atau tidak untuk sistem file Multi-AZ Anda tergantung pada metode yang Anda gunakan untuk mengakses data sistem file Anda. Sistem file single-AZ tidak memerlukan Transit Gateway. Tabel berikut menjelaskan kapan Anda perlu menggunakan AWS Transit Gateway untuk mengakses sistem file Multi-AZ.

Akses data	Membutuhkan Transit Gateway?
Mengakses FSx melalui NFS, SMB, atau ONTAP REST API, CLI atau NetApp BlueXP	Hanya jika: • Mengakses dari jaringan peered (lokal, misalnya), dan

Akses data	Membutuhkan Transit Gateway?
	• Anda tidak mengakses FSx melalui NetApp FlexCache instance Cache File Global atau Global
Mengakses data melalui iSCSI	Tidak
Bergabung dengan SVM ke Active Directory	Tidak
SnapMirror	Tidak
FlexCache Caching	Tidak
Cache File Global	Tidak

Mengkonfigurasi routing menggunakan AWS Transit Gateway

Jika Anda memiliki sistem file Multi-AZ dengan `EndpointIPAddressRange` yang berada di luar jangkauan CIDR VPC Anda, Anda perlu mengatur perutean tambahan AWS Transit Gateway untuk mengakses sistem file Anda dari jaringan peered atau lokal.

Important

Untuk mengakses sistem file Multi-AZ menggunakan Transit Gateway, setiap lampiran Transit Gateway harus dibuat dalam subnet yang tabel rutenya dikaitkan dengan sistem file Anda.

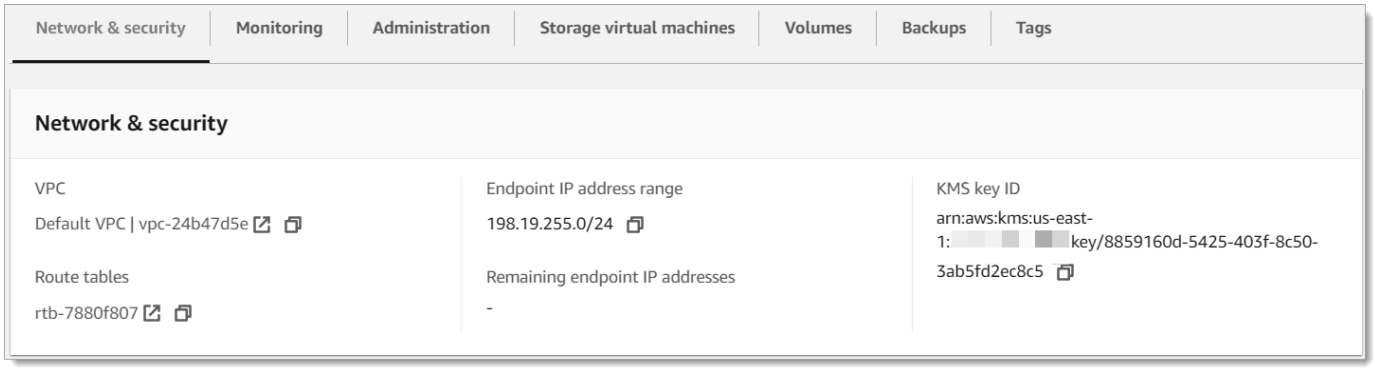
Note

Tidak diperlukan konfigurasi Transit Gateway tambahan untuk sistem file Single-AZ atau sistem file Multi-AZ dengan `EndpointIPAddressRange` yang berada dalam rentang alamat IP VPC Anda.

Untuk mengkonfigurasi routing menggunakan AWS Transit Gateway

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.

2. Pilih fsX untuk sistem file ONTAP yang Anda konfigurasi akses dari jaringan peered.
3. Dalam Jaringan & keamanan salin rentang alamat IP Endpoint.



4. Tambahkan rute ke Transit Gateway yang merutekan lalu lintas yang ditujukan untuk rentang alamat IP ini ke VPC sistem file Anda. Untuk informasi selengkapnya, lihat Bekerja dengan gateway transit di Gateway Transit VPC Amazon.
5. Konfirmasikan bahwa Anda dapat mengakses FSx Anda untuk sistem file ONTAP dari jaringan peered.

Untuk menambahkan tabel rute ke sistem file Anda, lihatMemperbarui sistem file.

> **Note**
>
> Catatan DNS untuk manajemen, NFS, dan titik akhir SMB hanya dapat diselesaikan dari dalam VPC yang sama dengan sistem file. Untuk memasang volume atau terhubung ke port manajemen dari jaringan lain, Anda perlu menggunakan alamat IP titik akhir. Alamat IP ini tidak berubah seiring waktu.

Mengakses iSCSI atau titik akhir antar-cluster di luar VPC penerapan

Anda dapat menggunakan VPC Peering atau AWS Transit Gateway untuk mengakses iSCSI sistem file Anda atau titik akhir antar-cluster dari luar VPC penyebaran sistem file. Anda dapat menggunakan VPC Peering untuk merutekan iSCSI dan lalu lintas antar-cluster antar VPC. Koneksi peering VPC adalah koneksi jaringan antara dua VPC, dan digunakan untuk merutekan lalu lintas di antara mereka menggunakan alamat IPv4 pribadi. Anda dapat menggunakan VPC peering untuk menghubungkan VPC dalam hal yang sama Wilayah AWS atau di antara yang berbeda. Wilayah AWS Untuk informasi lebih lanjut tentang peering VPC, lihat Apa itu VPC peering? di Panduan Peering VPC Amazon.

Mengakses data dari lokal

Anda dapat mengakses FSx untuk sistem file ONTAP dari lokal menggunakan AWS VPNdan AWS Direct Connect; pedoman kasus penggunaan yang lebih spesifik tersedia di bagian berikut. Selain persyaratan apa pun yang tercantum di bawah ini untuk mengakses FSx yang berbeda untuk sumber daya ONTAP dari lokal, Anda juga perlu memastikan bahwa grup keamanan VPC sistem file Anda memungkinkan data mengalir antara sistem file dan klien Anda; untuk daftar port yang diperlukan, lihat grup keamanan VPC Amazon.

Mengakses NFS, SMB, atau titik akhir ONTAP CLI atau REST API dari lokal

Bagian ini menjelaskan cara mengakses port manajemen NFS, SMB, dan ONTAP di fsX untuk sistem file ONTAP dari jaringan lokal.

Mengakses sistem file Multi-AZ

Amazon FSx mengharuskan Anda menggunakan AWS Transit Gateway atau mengonfigurasi Cache File NetApp Global jarak jauh atau NetApp FlexCache mengakses sistem file multi-AZ dari jaringan lokal. Untuk mendukung failover di seluruh AZ untuk sistem file multi-AZ, Amazon FSx menggunakan alamat IP mengambang untuk antarmuka yang digunakan untuk titik akhir manajemen NFS, SMB, dan ONTAP. Karena titik akhir NFS, SMB, dan manajemen menggunakan IP mengambang, Anda harus menggunakan AWS Transit Gatewaybersama dengan AWS Direct Connect atau AWS VPN untuk mengakses antarmuka ini dari jaringan lokal. Alamat IP mengambang yang digunakan untuk antarmuka ini berada di dalam yang `EndpointIpAddressRange` Anda tentukan saat membuat sistem file Multi-AZ Anda. Jika Anda membuat sistem file dari konsol Amazon FSx, secara default Amazon fsX memilih 64 alamat IP terakhir dari rentang CIDR utama VPC untuk digunakan sebagai rentang alamat IP titik akhir untuk sistem file. Jika Anda membuat sistem file dari AWS CLI atau Amazon FSx API, secara default Amazon fsX memilih rentang alamat IP dari dalam rentang alamat IP. `198.19.0.0/16` Alamat IP mengambang digunakan untuk memungkinkan transisi mulus klien Anda ke sistem file siaga jika failover diperlukan. Untuk informasi selengkapnya, lihat Proses failover untuk FSx untuk ONTAP.

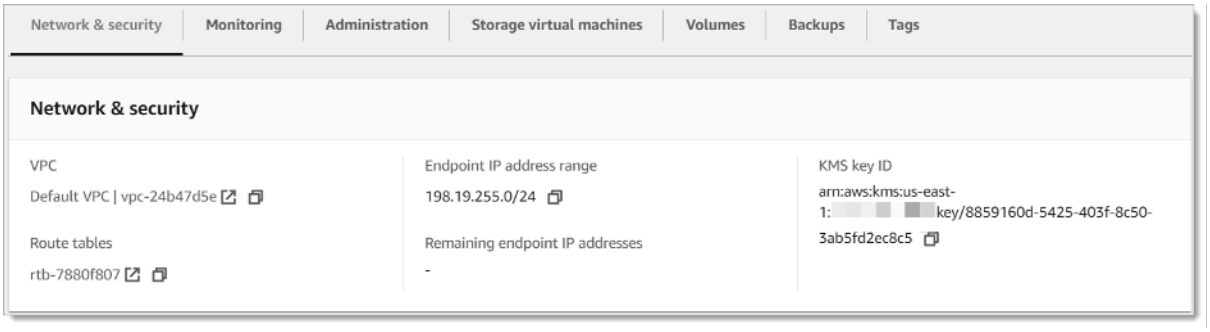
> **Important**
>
> Untuk mengakses sistem file Multi-AZ menggunakan Transit Gateway, setiap lampiran Transit Gateway harus dibuat dalam subnet yang tabel rutenya dikaitkan dengan sistem file Anda.

AWS Transit Gateway Untuk mengonfigurasi akses dari luar VPC Anda

Jika Anda memiliki sistem file Multi-AZ dengan `EndpointIPAddressRange` yang berada di luar jangkauan CIDR VPC Anda, Anda perlu mengatur perutean tambahan AWS Transit Gateway untuk mengakses sistem file Anda dari jaringan peered atau lokal.

> **Note**
>
> Tidak diperlukan konfigurasi Transit Gateway tambahan untuk sistem file Single-AZ atau sistem file Multi-AZ dengan `EndpointIPAddressRange` yang berada dalam rentang alamat IP VPC Anda.

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Pilih fsX untuk sistem file ONTAP yang Anda konfigurasi akses dari jaringan peered.
3. Di Jaringan & keamanan salin rentang alamat IP Endpoint.



4. Tambahkan rute ke Transit Gateway yang merutekan lalu lintas yang ditujukan untuk rentang alamat IP ini ke VPC sistem file Anda. Untuk informasi selengkapnya, lihat Bekerja dengan gateway transit di Panduan Pengguna Gateway Transit VPC Amazon.
5. Konfirmasikan bahwa Anda dapat mengakses FSx Anda untuk sistem file ONTAP dari jaringan peered.

> **Important**
>
> Untuk mengakses sistem file Multi-AZ menggunakan Transit Gateway, setiap lampiran Transit Gateway harus dibuat dalam subnet yang tabel rutenya dikaitkan dengan sistem file Anda.

Untuk menambahkan tabel rute ke sistem file Anda, lihatMemperbarui sistem file.

Mengakses sistem file Single-AZ

Persyaratan yang digunakan AWS Transit Gateway untuk mengakses data dari jaringan lokal tidak ada untuk sistem file Single-AZ. Sistem file single-AZ digunakan dalam satu subnet, dan alamat IP mengambang tidak diperlukan untuk menyediakan failover antar node. Sebaliknya, alamat IP yang Anda akses pada sistem file Single-AZ diimplementasikan sebagai alamat IP sekunder dalam rentang CIDR VPC sistem file, memungkinkan Anda untuk mengakses data Anda dari jaringan lain tanpa memerlukan. AWS Transit Gateway

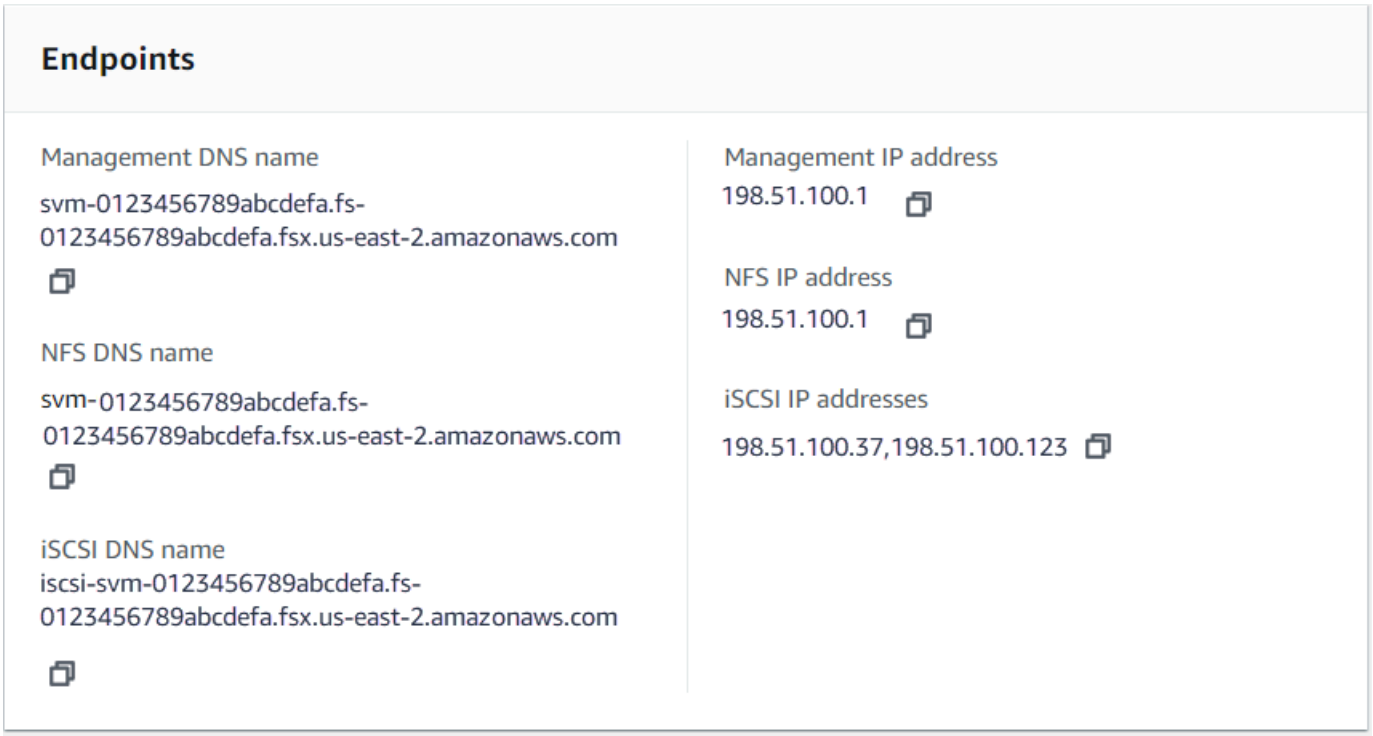
Mengakses titik akhir antar-cluster dari lokal

FSx untuk titik akhir antar-cluster ONTAP didedikasikan untuk lalu lintas replikasi antara sistem file ONTAP, termasuk antara penerapan lokal dan fsX untuk NetApp ONTAP. NetApp Lalu lintas replikasi mencakup SnapMirror, FlexCache, dan FlexClone hubungan antara mesin virtual penyimpanan (SVM) dan volume di berbagai sistem file, dan Cache File NetApp Global. Endpoint antar-cluster juga digunakan untuk lalu lintas Active Directory.

Karena titik akhir antar-kluster sistem file menggunakan alamat IP yang berada dalam rentang CIDR dari VPC yang Anda berikan saat Anda membuat fsX untuk sistem file ONTAP, Anda tidak diharuskan menggunakan Gateway Transit untuk merutekan lalu lintas antar klaster antara lokal dan. AWS Cloud Namun, klien lokal tetap harus menggunakan AWS VPN atau AWS Direct Connect membuat koneksi aman ke VPC Anda.

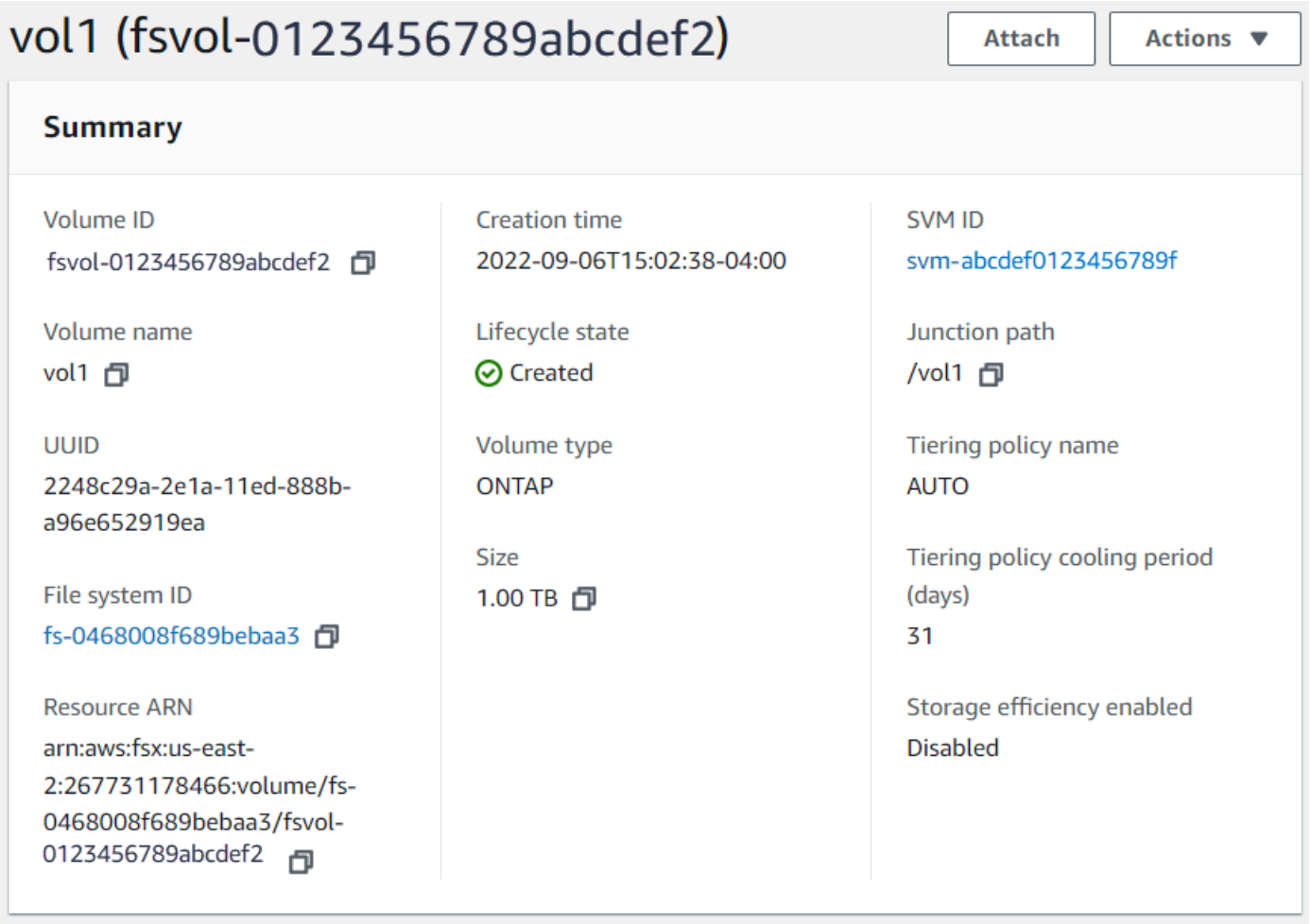
Volume pemasangan

Anda mengakses data di FSx untuk ONTAP dengan memasang volume pada klien Anda. Perintah di bagian ini menggunakan nama DNS atau alamat IP SVM di mana volume dibuat untuk memasang atau melampirkan volume. Anda dapat menemukan nama DNS dan alamat IP SVM di konsol Amazon FSx dengan memilih ONTAP > Mesin virtual penyimpanan, atau pada tab Mesin virtual Penyimpanan di halaman detail sistem file untuk sistem file, yang ditunjukkan pada gambar berikut.



Atau, Anda dapat menemukannya dalam respons operasi DescribeStorageVirtualMachinesAPI.

Anda dapat menemukan jalur persimpangan volume di konsol Amazon FSx pada panel Ringkasan halaman detail volume, yang ditunjukkan pada gambar berikut.



Topik

- Pemasangan pada klien Linux
- Pemasangan pada klien Microsoft Windows
- Memasang pada klien macOS

Pemasangan pada klien Linux

Kami merekomendasikan bahwa volume SVM yang Anda lampirkan klien Linux memiliki pengaturan gaya keamanan atau. `UNIX` `mixed` Untuk informasi selengkapnya, lihat Mengelola FSx untuk volume ONTAP.

> **Note**
>
> Secara default, fsX untuk pemasangan NFS ONTAP adalah mount. `hard` Untuk memastikan failover yang lancar jika terjadi, kami sarankan Anda menggunakan opsi `hard` pemasangan default.

Untuk memasang volume ONTAP pada klien Linux

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Buat atau pilih instans Amazon EC2 yang menjalankan Amazon Linux 2 yang berada di VPC yang sama dengan sistem file.

   Untuk informasi selengkapnya tentang meluncurkan instans EC2 Linux, lihat Langkah 1: Meluncurkan instans di Panduan Pengguna Amazon EC2.
3. Connect ke instans Amazon EC2 Linux Anda. Untuk informasi selengkapnya, lihat Connect ke instans Linux Anda di Panduan Pengguna Amazon EC2.
4. Buka terminal pada instans EC2 Anda menggunakan shell aman (SSH), dan masuk dengan kredensi yang sesuai.
5. Buat direktori pada instans EC2 untuk memasang volume SVM sebagai berikut:

   ```
   sudo mkdir /fsx
   ```
6. Pasang volume ke direktori yang baru saja Anda buat menggunakan perintah berikut:

   ```
   sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
   ```

   Contoh berikut menggunakan nilai sampel.

   ```
   sudo mount -t nfs svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-
   east-1.amazonaws.com:/vol1 /fsx
   ```

   Anda juga dapat menggunakan SVM alamat IP SVM alih-alih nama DNS-nya. Sebaiknya gunakan nama DNS untuk memasang klien ke sistem file skala karena membantu memastikan bahwa klien Anda seimbang di seluruh pasangan ketersediaan tinggi (HA) sistem file Anda.

   ```
   sudo mount -t nfs 198.51.100.1:/vol1 /fsx
   ```

> **Note**
>
> Untuk sistem file scale-out, protokol paralel NFS (PNFS) diaktifkan secara default dan digunakan secara default untuk setiap klien yang memasang volume dengan NFS v4.1 atau lebih besar.

Menggunakan /etc/fstab untuk me-mount secara otomatis saat reboot instance

Untuk secara otomatis menyalakan ulang FSx Anda untuk volume ONTAP saat instans Amazon EC2 Linux reboot, gunakan file tersebut. `/etc/fstab` File `/etc/fstab` berisi informasi tentang sistem file. Perintah`mount -a`, yang berjalan selama start-up instance, memasang sistem file yang terdaftar di. `/etc/fstab`

> **Note**
>
> FSx untuk sistem file ONTAP tidak mendukung pemasangan otomatis menggunakan instans Amazon `/etc/fstab` EC2 Mac.

> **Note**
>
> Sebelum Anda dapat memperbarui `/etc/fstab` file instans EC2 Anda, pastikan bahwa Anda sudah membuat fsX Anda untuk sistem file ONTAP. Untuk informasi selengkapnya, lihat Membuat fsX untuk sistem file ONTAP.

Untuk memperbarui berkas /etc/fstab pada instans EC2 Anda

1. Connect ke instans EC2 Anda:
   - Untuk menyambung ke instans Anda dari komputer yang menjalankan macOS atau Linux, tentukan file.pem untuk perintah SSH Anda. Untuk melakukan ini, gunakan `-i` opsi dan jalur ke kunci pribadi Anda.
   - Untuk terhubung ke instans Anda dari komputer yang menjalankan Windows, Anda dapat menggunakan MindTerm atau PuTTY. Untuk menggunakan PuTTY, instal dan konversi file.pem ke file.ppk.

Untuk informasi selengkapnya, lihat topik berikut di Panduan Pengguna Amazon EC2:

- Menghubungkan ke instans Linux Anda menggunakan SSH
- Menghubungkan ke instans Linux Anda dari Windows menggunakan PuTTY

2. Buat direktori lokal yang akan digunakan untuk me-mount volume SVM.

```
sudo mkdir /fsx
```

3. Buka `/etc/fstab` file di editor pilihan Anda.
4. Tambahkan baris berikut ke file `/etc/fstab`. Masukkan karakter tab di antara setiap parameter. Ini akan muncul sebagai satu baris tanpa jeda baris.

```
svm-dns-name:volume-junction-path /fsx nfs nfsvers=version,defaults 0 0
```

Anda juga dapat menggunakan alamat IP SVM volume. Tiga parameter terakhir menunjukkan opsi NFS (yang kami atur ke default), pembuangan sistem file dan pemeriksaan sistem file (ini biasanya tidak digunakan sehingga kami mengaturnya ke 0).

5. Simpan perubahan pada file.
6. Sekarang pasang file share menggunakan perintah berikut. Lain kali sistem dimulai, folder akan dipasang secara otomatis.

```
sudo mount /fsx
sudo mount svm-dns-name:volume-junction-path
```

Instans EC2 Anda sekarang dikonfigurasi untuk memasang volume ONTAP setiap kali dimulai ulang.

Pemasangan pada klien Microsoft Windows

Bagian ini menjelaskan cara mengakses data di FSx Anda untuk sistem file ONTAP dengan klien yang menjalankan sistem operasi Microsoft Windows. Tinjau persyaratan berikut, terlepas dari jenis klien yang Anda gunakan.

Prosedur ini mengasumsikan bahwa klien dan sistem file terletak di Akun AWS VPC yang sama dan. Jika klien berada di lokasi atau di VPC yang berbeda,, atau Akun AWS Wilayah AWS, prosedur ini juga mengasumsikan bahwa Anda telah menyiapkan AWS Transit Gateway atau koneksi jaringan

khusus menggunakan AWS Direct Connect atau menggunakan terowongan pribadi yang aman. AWS Virtual Private Network Untuk informasi selengkapnya, lihat Mengakses data dari luar VPC penyebaran.

Kami menyarankan Anda melampirkan volume ke klien Windows Anda menggunakan protokol SMB.

Prasyarat

Untuk mengakses volume penyimpanan ONTAP menggunakan klien Microsoft Windows, Anda harus memenuhi prasyarat berikut:

- SVM volume yang Anda lampirkan harus digabungkan ke Active Directory organisasi Anda, atau Anda harus menggunakan workgroup. Untuk informasi selengkapnya tentang menggabungkan SVM Anda ke Active Directory, lihatMengelola fsX untuk mesin virtual penyimpanan ONTAP. Untuk informasi selengkapnya tentang penggunaan workgroup, lihat Menyiapkan server SMB dalam ikhtisar workgroup di Pusat NetApp Dokumentasi.
- Volume yang Anda lampirkan memiliki pengaturan gaya keamanan `NTFS` atau`mixed`. Untuk informasi selengkapnya, lihat Mengelola FSx untuk volume ONTAP.

Untuk melampirkan volume ONTAP pada klien Windows menggunakan SMB dan Active Directory

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Buat atau pilih instans Amazon EC2 yang menjalankan Microsoft Windows yang berada di VPC yang sama dengan sistem file, dan bergabung ke Microsoft Active Directory yang sama dengan SVM volume.

   Untuk informasi selengkapnya tentang meluncurkan instans, lihat Langkah 1: Meluncurkan instans di Panduan Pengguna Amazon EC2.

   Untuk informasi selengkapnya tentang menggabungkan SVM ke Active Directory, lihatMengelola fsX untuk mesin virtual penyimpanan ONTAP.
3. Connect ke instans Windows Amazon EC2 Anda. Untuk informasi selengkapnya, lihat Menyambungkan ke instans Windows Anda di Panduan Pengguna Amazon EC2.
4. Buka prompt perintah.
5. Jalankan perintah berikut. Ganti yang berikut ini:

   - Ganti `Z:` dengan huruf drive yang tersedia.
   - Ganti `DNS_NAME` dengan nama DNS atau alamat IP titik akhir SMB untuk SVM volume.

- Ganti `SHARE_NAME` dengan nama saham SMB. `C$`adalah pangsa SMB default di root namespace SVM, tetapi Anda tidak boleh memasangnya karena itu memperlihatkan penyimpanan ke volume root dan dapat menyebabkan gangguan keamanan dan layanan. Anda harus memberikan nama berbagi SMB untuk dipasang, bukan. `C$` Untuk informasi selengkapnya tentang membuat saham SMB, lihatMengelola saham SMB.

```
net use Z: \\DNS_NAME\SHARE_NAME
```

Contoh berikut menggunakan nilai sampel.

```
net use Z: \\corp.example.com\group_share
```

Anda juga dapat menggunakan alamat IP SVM alih-alih nama DNS-nya. Sebaiknya gunakan nama DNS untuk memasang klien ke sistem file skala karena membantu memastikan bahwa klien Anda seimbang di seluruh pasangan ketersediaan tinggi (HA) sistem file Anda.

```
net use Z: \\198.51.100.5\group_share
```

Memasang pada klien macOS

Bagian ini menjelaskan cara mengakses data di FSx Anda untuk sistem file ONTAP dengan klien yang menjalankan sistem operasi macOS. Tinjau persyaratan berikut, terlepas dari jenis klien yang Anda gunakan.

Prosedur ini mengasumsikan bahwa klien dan sistem file terletak di Akun AWS VPC yang sama dan. Jika klien berada di lokasi, atau di VPC yang berbeda, atau Wilayah AWS, Anda telah menyiapkan Akun AWS atau koneksi jaringan khusus menggunakan AWS Transit Gateway AWS Direct Connect atau menggunakan terowongan pribadi yang aman. AWS Virtual Private Network Untuk informasi selengkapnya, lihat Mengakses data dari luar VPC penyebaran.

Kami menyarankan Anda melampirkan volume ke klien Mac Anda menggunakan protokol SMB.

Untuk memasang volume ONTAP pada klien macOS menggunakan SMB

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.

2. Buat atau pilih instans Amazon EC2 Mac yang menjalankan macOS yang ada di VPC yang sama dengan sistem file.

   Untuk informasi selengkapnya tentang meluncurkan instans, lihat Langkah 1: Meluncurkan instans di Panduan Pengguna Amazon EC2.

3. Connect ke instans Amazon EC2 Mac Anda. Untuk informasi selengkapnya, lihat Connect ke instans Linux Anda di Panduan Pengguna Amazon EC2.

4. Buka terminal pada instans EC2 Anda menggunakan shell aman (SSH), dan masuk dengan kredensi yang sesuai.

5. Buat direktori pada instans EC2 untuk memasang volume sebagai berikut:

   ```
   sudo mkdir /fsx
   ```

6. Pasang volume menggunakan perintah berikut.

   ```
   sudo mount -t smbfs filesystem-dns-name:/smb-share-name mount-point
   ```

   Contoh berikut menggunakan nilai sampel.

   ```
   sudo mount -t smbfs svm-01234567890abcde2.fs-01234567890abcde5.fsx.us-
   east-1.amazonaws.com:/C$ /fsx
   ```

   Anda juga dapat menggunakan alamat IP SVM alih-alih nama DNS-nya. Sebaiknya gunakan nama DNS untuk memasang klien ke sistem file skala karena membantu memastikan bahwa klien Anda seimbang di seluruh pasangan ketersediaan tinggi (HA) sistem file Anda.

   ```
   sudo mount -t smbfs 198.51.100.10:/C$ /fsx
   ```

   `C$`adalah berbagi SMB default yang dapat Anda pasang untuk melihat root namespace SVM. Jika Anda telah membuat pembagian Blok Pesan Server (SMB) apa pun di SVM Anda, berikan nama berbagi SMB sebagai gantinya. `C$` Untuk informasi selengkapnya tentang membuat saham SMB, lihatMengelola saham SMB.

Untuk memasang volume ONTAP pada klien macOS menggunakan NFS

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.

2. Buat atau pilih instans Amazon EC2 yang menjalankan Amazon Linux 2 yang berada di VPC yang sama dengan sistem file.

   Untuk informasi selengkapnya tentang meluncurkan instans EC2 Linux, lihat Langkah 1: Meluncurkan instans di Panduan Pengguna Amazon EC2.

3. Connect ke instans Amazon EC2 Linux Anda. Untuk informasi selengkapnya, lihat Connect ke instans Linux Anda di Panduan Pengguna Amazon EC2.

4. Pasang FSx Anda untuk volume ONTAP pada instans Linux EC2 dengan menggunakan skrip data pengguna selama peluncuran instance, atau dengan menjalankan perintah berikut:

   ```
   sudo mount -t nfs -o nfsvers=NFS_version svm-dns-name:/volume-junction-path /mount-point
   ```

   Contoh berikut menggunakan nilai sampel.

   ```
   sudo mount -t nfs -o nfsvers=4.1
    svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /
   fsxontap
   ```

   Anda juga dapat menggunakan SVM alamat IP SVM alih-alih nama DNS-nya. Sebaiknya gunakan nama DNS untuk memasang klien ke sistem file skala karena membantu memastikan bahwa klien Anda seimbang di seluruh pasangan HA sistem file Anda.

   ```
   sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
   ```

5. Pasang volume ke direktori yang baru saja Anda buat menggunakan perintah berikut.

   ```
   sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
   ```

   Contoh berikut menggunakan nilai sampel.

   ```
   sudo mount -t nfs svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-
   east-1.amazonaws.com:/vol1 /fsx
   ```

   Anda juga dapat menggunakan SVM alamat IP SVM alih-alih nama DNS-nya. Sebaiknya gunakan nama DNS untuk memasang klien ke sistem file skala karena membantu memastikan bahwa klien Anda seimbang di seluruh pasangan ketersediaan tinggi (HA) sistem file Anda.

```
sudo mount -t nfs 198.51.100.1:/vol1 /fsx
```

Memasang iSCSI LUN

Amazon fsX untuk NetApp ONTAP menyediakan dukungan penyimpanan blok bersama melalui protokol iSCSI (Internet Small Computer Systems Interface). Anda dapat mengaktifkan penyimpanan iSCSI dengan menyediakan LUN (Logical Unit Number) dan memetakannya ke grup inisiator (igroups), mengekspos penyimpanan blok ke host Linux dan Windows Anda.

> **Note**
>
> Protokol iSCSI tidak didukung untuk fsX untuk sistem file scale-out ONTAP, yang merupakan sistem file dengan lebih dari satu pasangan server file ketersediaan tinggi (HA).

Topik

- Memasang iSCSI LUN ke klien Linux
- Memasang iSCSI LUN ke klien Windows

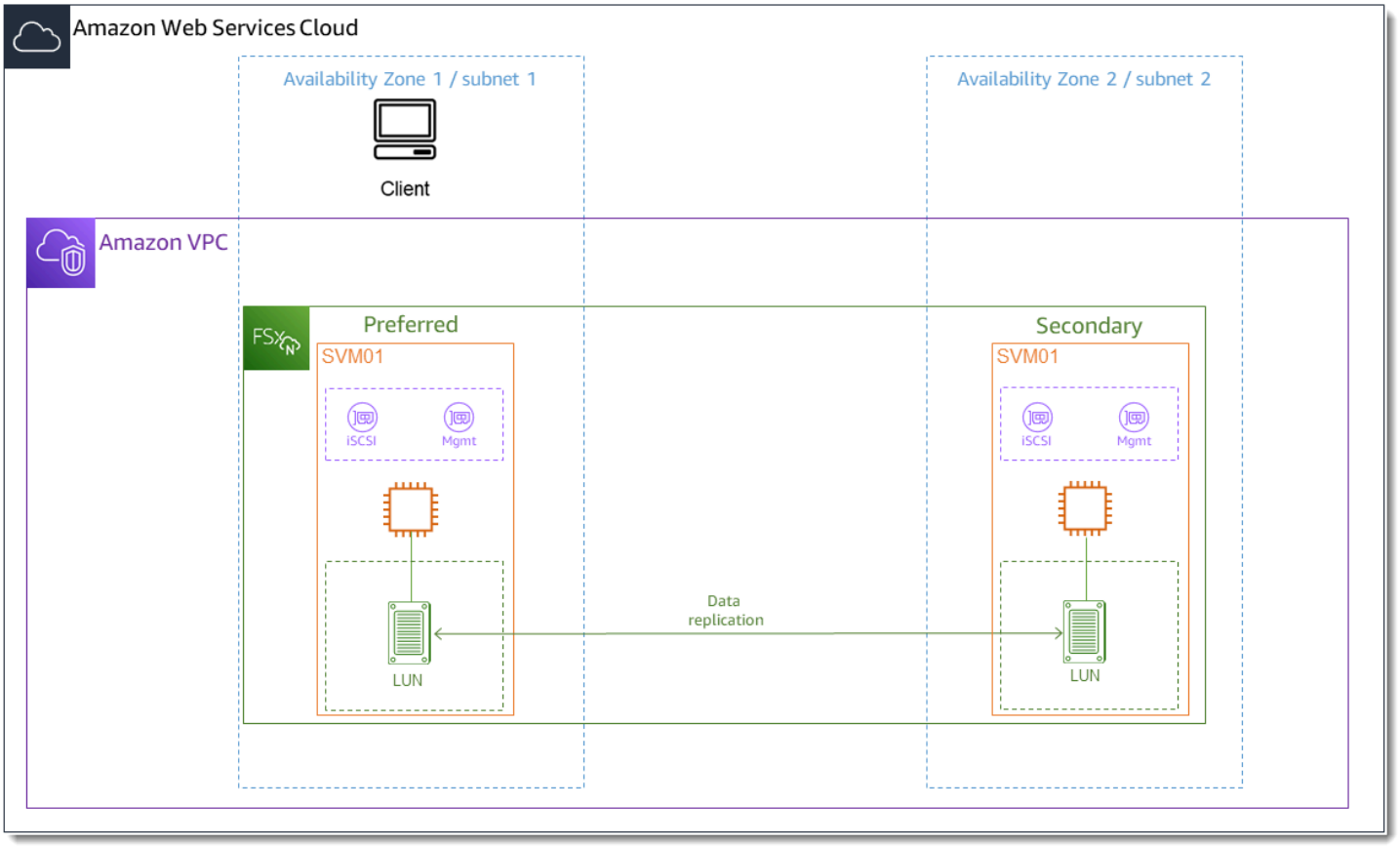
Memasang iSCSI LUN ke klien Linux

Contoh-contoh yang disajikan dalam prosedur ini menggunakan pengaturan berikut:

- ISCSI LUN yang sedang dipasang ke host Linux sudah dibuat. Untuk informasi selengkapnya, lihat Membuat iSCSI LUN.
- Host Linux yang memasang iSCSI LUN adalah instans Amazon EC2 yang menjalankan Amazon Linux 2 Amazon Machine Image (AMI). Ini memiliki grup keamanan VPC yang dikonfigurasi untuk memungkinkan lalu lintas masuk dan keluar seperti yang dijelaskan dalam. Kontrol Akses Sistem File dengan Amazon VPC
- Host Linux dan FSx untuk sistem file ONTAP terletak di VPC yang sama dan. Akun AWS Jika host berada di VPC lain, Anda dapat menggunakan VPC peering atau AWS Transit Gateway untuk memberikan VPC lain akses ke titik akhir iSCSI volume. Untuk informasi selengkapnya, lihat Mengakses data dari luar VPC penyebaran.

Jika Anda menggunakan instans EC2 yang menjalankan AMI Linux yang berbeda, beberapa utilitas yang diinstal pada host mungkin sudah diinstal sebelumnya, dan Anda mungkin menggunakan perintah yang berbeda untuk menginstal paket yang diperlukan. Selain menginstal paket, perintah yang digunakan di bagian ini berlaku untuk AMI Linux EC2 lainnya.

Sebaiknya instans EC2 berada di zona ketersediaan yang sama dengan subnet pilihan sistem file Anda, seperti yang ditunjukkan pada grafik berikut.



Topik

- Instal dan konfigurasikan iSCSI pada klien Linux
- Konfigurasikan iSCSI pada fsX untuk sistem file ONTAP
- Pasang iSCSI LUN di klien Linux Anda

Instal dan konfigurasikan iSCSI pada klien Linux

Untuk menginstal klien iSCSI

1. Konfirmasikan `device-mapper-multipath` itu `iscsi-initiator-utils` dan diinstal pada perangkat Linux Anda. Connect ke instance Linux Anda menggunakan klien SSH. Untuk informasi selengkapnya, lihat Connect ke instans Linux menggunakan SSH.
2. Instal `multipath` dan klien iSCSI menggunakan perintah berikut. Instalasi `multipath` diperlukan jika Anda ingin secara otomatis failover antara server file Anda.

```
~$ sudo yum install -y device-mapper-multipath iscsi-initiator-utils
```

3. Untuk memfasilitasi respons yang lebih cepat ketika secara otomatis gagal di antara server file saat menggunakan`multipath`, atur nilai batas waktu penggantian dalam `/etc/iscsi/iscsid.conf` file ke nilai 5 alih-alih menggunakan nilai default. `120`

```
~$ sudo sed -i 's/node.session.timeo.replacement_timeout = .*/
node.session.timeo.replacement_timeout = 5/' /etc/iscsi/iscsid.conf; sudo cat /etc/
iscsi/iscsid.conf | grep node.session.timeo.replacement_timeout
```

4. Mulai layanan iSCSI.

```
~$ sudo service iscsid start
```

   Perhatikan bahwa tergantung pada versi Linux Anda, Anda mungkin harus menggunakan perintah ini sebagai gantinya:

```
~$ sudo systemctl start iscsid
```

5. Konfirmasikan bahwa layanan sedang berjalan menggunakan perintah berikut.

```
~$ sudo systemctl status iscsid.service
```

   Sistem merespons dengan output berikut:

```
iscsid.service - Open-iSCSI
    Loaded: loaded (/usr/lib/systemd/system/iscsid.service; disabled; vendor
 preset: disabled)
    Active: active (running) since Fri 2021-09-02 00:00:00 UTC; 1min ago
```

```
    Docs: man:iscsid(8)
    man:iscsiadm(8)
    Process: 14658 ExecStart=/usr/sbin/iscsid (code=exited, status=0/SUCCESS)
    Main PID: 14660 (iscsid)
    CGroup: /system.slice/iscsid.service
    ##14659 /usr/sbin/iscsid
    ##14660 /usr/sbin/iscsid
```

Untuk mengkonfigurasi iSCSI pada klien Linux Anda

1. Untuk mengaktifkan klien Anda untuk secara otomatis failover antara server file Anda, Anda harus mengkonfigurasi multipath. Gunakan perintah berikut ini.

   ```
   ~$ sudo mpathconf --enable --with_multipathd y
   ```

2. Tentukan nama inisiator host Linux Anda menggunakan perintah berikut. Lokasi nama inisiator tergantung pada utilitas iSCSI Anda. Jika Anda menggunakan`iscsi-initiator-utils`, nama inisiator terletak di file`/etc/iscsi/initiatorname.iscsi`.

   ```
   ~$ sudo cat /etc/iscsi/initiatorname.iscsi
   ```

   Sistem merespons dengan nama inisiator.

   ```
   InitiatorName=iqn.1994-05.com.redhat:abcdef12345
   ```

Konfigurasikan iSCSI pada fsX untuk sistem file ONTAP

1. Connect ke NetApp ONTAP CLI pada fsX untuk sistem file ONTAP tempat Anda membuat iSCSI LUN menggunakan perintah berikut. Untuk informasi selengkapnya, lihat Menggunakan CLI NetApp ONTAP.

   ```
   ~$ ssh fsxadmin@your_management_endpoint_ip
   ```

2. Buat grup inisiator (`igroup`) menggunakan perintah NetApp ONTAP CLI. lun igroup create Grup inisiator memetakan ke iSCSI LUN dan mengontrol inisiator (klien) mana yang memiliki akses ke LUNs. Ganti `host_initiator_name` dengan nama inisiator dari host Linux Anda yang Anda ambil dalam prosedur sebelumnya.

```
::> lun igroup create -vserver svm_name -igroup igroup_name -
initiator host_initiator_name -protocol iscsi -ostype linux
```

Jika Anda ingin membuat LUN yang dipetakan ke igroup ini tersedia untuk beberapa host, Anda dapat menentukan beberapa nama inisiator yang dipisahkan dengan koma. Untuk informasi selengkapnya, lihat lun igroup create di Pusat Dokumentasi NetApp ONTAP.

3. Konfirmasikan bahwa `igroup` ada menggunakan lun igroup showperintah:

```
::> lun igroup show
```

Sistem merespons dengan output berikut:

```
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
svm_name  igroup_name  iscsi    linux    iqn.1994-05.com.redhat:abcdef12345
```

4. Langkah ini mengasumsikan bahwa Anda telah membuat iSCSI LUN. Jika belum, lihat step-by-step instruksi Membuat iSCSI LUN untuk melakukannya.

   Buat pemetaan dari LUN yang Anda buat ke igroup yang Anda buat, menggunakan lun mapping create, menentukan atribut berikut:

   - *svm_name*— Nama mesin virtual penyimpanan yang menyediakan target iSCSI. Tuan rumah menggunakan nilai ini untuk mencapai LUN.
   - *vol_name*— Nama volume hosting LUN.
   - *lun_name*— Nama yang Anda tetapkan ke LUN.
   - *igroup_name*— Nama grup inisiator.
   - *lun_id*— Bilangan bulat ID LUN khusus untuk pemetaan, bukan untuk LUN itu sendiri. Ini digunakan oleh inisiator di igroup sebagai Logical Unit Number menggunakan nilai ini untuk inisiator saat mengakses penyimpanan.

```
::> lun mapping create -vserver svm_name -path /vol/vol_name/lun_name -
igroup igroup_name -lun-id lun_id
```

5. Gunakan `lun show -path`perintah untuk mengonfirmasi LUN dibuat, online, dan dipetakan.

```
::> lun show -path /vol/vol_name/lun_name -fields state,mapped,serial-hex
```

Sistem merespons dengan output berikut:

```
 Vserver    Path                            serial-hex               state    mapped
 --------- ------------------------------- ------------------------ --------
 --------
 svm_name  /vol/vol_name/lun_name          6c5742314e5d52766e796150 online   mapped
```

Simpan `serial_hex` nilainya (dalam contoh ini`6c5742314e5d52766e796150`), Anda akan menggunakannya di langkah selanjutnya untuk membuat nama ramah untuk perangkat blok.

6. Gunakan `network interface show -vserver`perintah untuk mengambil alamat `iscsi_1` dan `iscsi_2` antarmuka untuk SVM di mana Anda telah membuat iSCSI LUN Anda.

```
::> network interface show -vserver svm_name
```

Sistem merespons dengan output berikut:

```
            Logical               Status     Network            Current
        Current Is
Vserver     Interface             Admin/Oper Address/Mask       Node
        Port    Home
----------- ----------            ---------- ------------------ -------------
        ------- ----
svm_name
            iscsi_1               up/up      172.31.0.143/20
 FSxId0123456789abcdef8-01  e0e     true
            iscsi_2               up/up      172.31.21.81/20
 FSxId0123456789abcdef8-02  e0e     true
            nfs_smb_management_1
                                  up/up      198.19.250.177/20
 FSxId0123456789abcdef8-01  e0e     true
3 entries were displayed.
```

Dalam contoh ini, alamat IP `iscsi_1` adalah `172.31.0.143` dan `iscsi_2` is`172.31.21.81`.

Pasang iSCSI LUN di klien Linux Anda

1. *Pada klien Linux Anda, gunakan perintah berikut untuk menemukan target IscSI node iscsi_1 menggunakan alamat IP iSCSI_1_IP.*

```
~$ sudo iscsiadm --mode discovery --op update --type sendtargets --
portal iscsi_1_IP
```

```
172.31.0.143:3260,1029
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3
172.31.21.81:3260,1028
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3
```

   Dalam contoh ini, `iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3` sesuai dengan untuk iSCSI LUN di zona ketersediaan yang disukai. `target_initiator`

2. (Opsional) Anda dapat membuat sesi tambahan dengan`target_initiator`. Amazon EC2 memiliki batas bandwidth 5 Gb/s (~ 625 MB/s) untuk lalu lintas aliran tunggal, tetapi Anda dapat membuat beberapa sesi untuk mendorong tingkat throughput yang lebih tinggi ke sistem file Anda dari satu klien. Untuk informasi selengkapnya, lihat Bandwidth jaringan instans Amazon EC2 di Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Linux.

   Perintah berikut menetapkan 8 sesi per inisiator per node ONTAP di setiap zona ketersediaan, memungkinkan klien untuk mendorong hingga 40 Gb/s (5.000 MB/s) throughput agregat ke iSCSI LUN.

```
~$ sudo iscsiadm --mode node -T target_initiator --op update -n
 node.session.nr_sessions -v 8
```

3. Masuk ke inisiator target. LUN iSCSI Anda disajikan sebagai disk yang tersedia.

```
~$ sudo iscsiadm --mode node -T target_initiator --login
```

```
Logging in to [iface: default, target:
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3, portal:
 172.31.14.66,3260] (multiple)
```

```
Login to [iface: default, target:
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3, portal:
 172.31.14.66,3260] successful.
```

Output di atas terpotong; Anda akan melihat satu `Logging in` dan satu `Login successful` respons untuk setiap sesi pada setiap server file. Dalam kasus 4 sesi per node, akan ada 8 `Logging in` dan 8 `Login successful` tanggapan.

4. Gunakan perintah berikut untuk memverifikasi bahwa `dm-multipath` telah mengidentifikasi dan menggabungkan sesi iSCSI dengan menampilkan LUN tunggal dengan beberapa kebijakan. Harus ada jumlah perangkat yang sama yang terdaftar sebagai `active` dan yang terdaftar sebagai`enabled`.

```
~$ sudo multipath -ll
```

Dalam output, nama disk diformat sebagai`dm-xyz`, di mana `xyz` adalah bilangan bulat. Jika tidak ada disk multipath lainnya, nilai ini adalah. `dm-0`

```
3600a09806c5742314e5d52766e79614f dm-xyz NETAPP  ,LUN C-Mode
size=10G features='4 queue_if_no_path pg_init_retries 50 retain_attached_hw_handle'
 hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| |- 0:0:0:1 sda     8:0   active ready running
| |- 1:0:0:1 sdc     8:32  active ready running
| |- 3:0:0:1 sdg     8:96  active ready running
| `- 4:0:0:1 sdh     8:112 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- 2:0:0:1 sdb     8:16  active ready running
  |- 7:0:0:1 sdf     8:80  active ready running
  |- 6:0:0:1 sde     8:64  active ready running
  `- 5:0:0:1 sdd     8:48  active ready running
```

Perangkat blok Anda sekarang terhubung ke klien Linux Anda. Itu terletak di bawah jalan setapak`/dev/dm-xyz`. Anda tidak boleh menggunakan jalur ini untuk tujuan administratif; sebagai gantinya, gunakan tautan simbolis yang berada di bawah jalur`/dev/mapper/wwid`, di mana *`wwid`* adalah pengenal unik untuk LUN Anda yang konsisten di seluruh perangkat. Pada langkah berikutnya, Anda akan memberikan nama yang ramah *`wwid`* sehingga Anda dapat membedakannya dari disk multipathed lainnya.

Untuk memberi perangkat blokir Anda nama yang ramah

1. Untuk memberikan nama yang ramah pada perangkat Anda, buat alias dalam `/etc/multipath.conf` file. Untuk melakukan ini, tambahkan entri berikut ke file menggunakan editor teks pilihan Anda, ganti placeholder berikut:

   - Ganti `serial_hex` dengan nilai yang Anda simpan dalam Konfigurasikan iSCSI pada fsX untuk sistem file ONTAP prosedur.
   - Tambahkan awalan `3600a0980` ke `serial_hex` nilai seperti yang ditunjukkan pada contoh. Ini adalah pembukaan unik untuk distribusi ONTAP yang digunakan Amazon FSx untuk NetApp ONTAP. NetApp
   - Ganti `device_name` dengan nama ramah yang ingin Anda gunakan untuk perangkat Anda.

```
multipaths {
    multipath {
        wwid 3600a0980serial_hex
        alias device_name
    }
}
```

Sebagai alternatif, Anda dapat menyalin dan menyimpan skrip berikut sebagai file bash, sepertimultipath_alias.sh. Anda dapat menjalankan skrip dengan hak istimewa sudo, mengganti *serial_hex* (tanpa awalan 3600a0980) dan *device_name* dengan nomor seri masing-masing dan nama ramah yang diinginkan. Skrip ini mencari `multipaths` bagian yang tidak dikomentari dalam file. `/etc/multipath.conf` Jika ada, itu menambahkan `multipath` entri ke bagian itu; jika tidak, itu akan membuat `multipaths` bagian baru dengan `multipath` entri untuk perangkat blok Anda.

```
#!/bin/bash
SN=serial_hex
ALIAS=device_name
CONF=/etc/multipath.conf
grep -q '^multipaths {' $CONF
UNCOMMENTED=$?
if [ $UNCOMMENTED -eq 0 ]
then
        sed -i '/^multipaths {/a\\tmultipath {\n\t\twwid 3600a0980'"${SN}"'\n\t
\talias '"${ALIAS}"'\n\t}\n' $CONF
else
```

```
        printf "multipaths {\n\tmultipath {\n\t\twwid 3600a0980$SN\n\t\talias
 $ALIAS\n\t}\n}" >> $CONF
fi
```

2. Mulai ulang `multipathd` layanan `/etc/multipathd.conf` agar perubahan diterapkan.

```
~$ systemctl restart multipathd.service
```

Untuk mempartisi LUN

Langkah selanjutnya adalah memformat dan mempartisi LUN Anda menggunakan`fdisk`.

1. Gunakan perintah berikut untuk memverifikasi bahwa jalur ke Anda `device_name` ada.

```
~$ ls /dev/mapper/device_name
```

```
/dev/device_name
```

2. Partisi disk menggunakan`fdisk`. Anda akan memasukkan prompt interaktif. Masukkan opsi dalam urutan yang ditampilkan. Perhatikan bahwa `Last sector` nilainya akan bervariasi tergantung pada ukuran iSCSI LUN Anda (10GB dalam contoh ini). Anda dapat membuat beberapa partisi dengan menggunakan nilai yang lebih kecil dari sektor terakhir (20971519dalam contoh ini).

```
~$ sudo fdisk /dev/mapper/device_name
```

Prompt `fsdisk` interaktif dimulai.

```
Welcome to fdisk (util-linux 2.30.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0x66595cb0.

Command (m for help): n
Partition type
   p primary (0 primary, 0 extended, 4 free)
   e extended (container for logical partitions)
```

```
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048): 2048
Last sector, +sectors or +size{K,M,G,T,P} (2048-20971519, default
 20971519): 20971519

Created a new partition 1 of type 'Linux' and of size 512 B.
Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.
```

Setelah masukw, partisi baru Anda `/dev/mapper/`*`partition_name`* menjadi tersedia. *`Partision_name memiliki format`* <device_name><partition_number>. 1digunakan sebagai nomor partisi yang digunakan dalam `fdisk` perintah pada langkah sebelumnya.

3. Buat sistem file Anda menggunakan `/dev/mapper/`*`partition_name`* sebagai jalur.

```
~$ sudo mkfs.ext4 /dev/mapper/partition_name
```

Sistem merespons dengan output berikut:

```
mke2fs 1.42.9 (28-Dec-2013)
Discarding device blocks: done
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=16 blocks
655360 inodes, 2621184 blocks
131059 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
80 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
     32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632
Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

Untuk me-mount LUN pada klien Linux

1. Buat direktori *directory_path* sebagai titik pemasangan untuk sistem file Anda.

```
~$ sudo mkdir /directory_path/mount_point
```

2. Pasang sistem file menggunakan perintah berikut.

```
~$ sudo mount -t ext4 /dev/mapper/partition_name /directory_path/mount_point
```

3. (Opsional) Anda dapat mengubah kepemilikan direktori mount ke pengguna Anda. Ganti *username* dengan nama pengguna Anda.

```
~$ sudo chown username:username /directory_path/mount_point
```

4. (Opsional) Verifikasi bahwa Anda dapat membaca dari dan menulis data ke sistem file.

```
~$ echo "Hello world!" > /directory_path/mount_point/HelloWorld.txt
~$ cat directory_path/HelloWorld.txt
Hello world!
```

Anda telah berhasil membuat dan memasang iSCSI LUN pada klien Linux Anda.

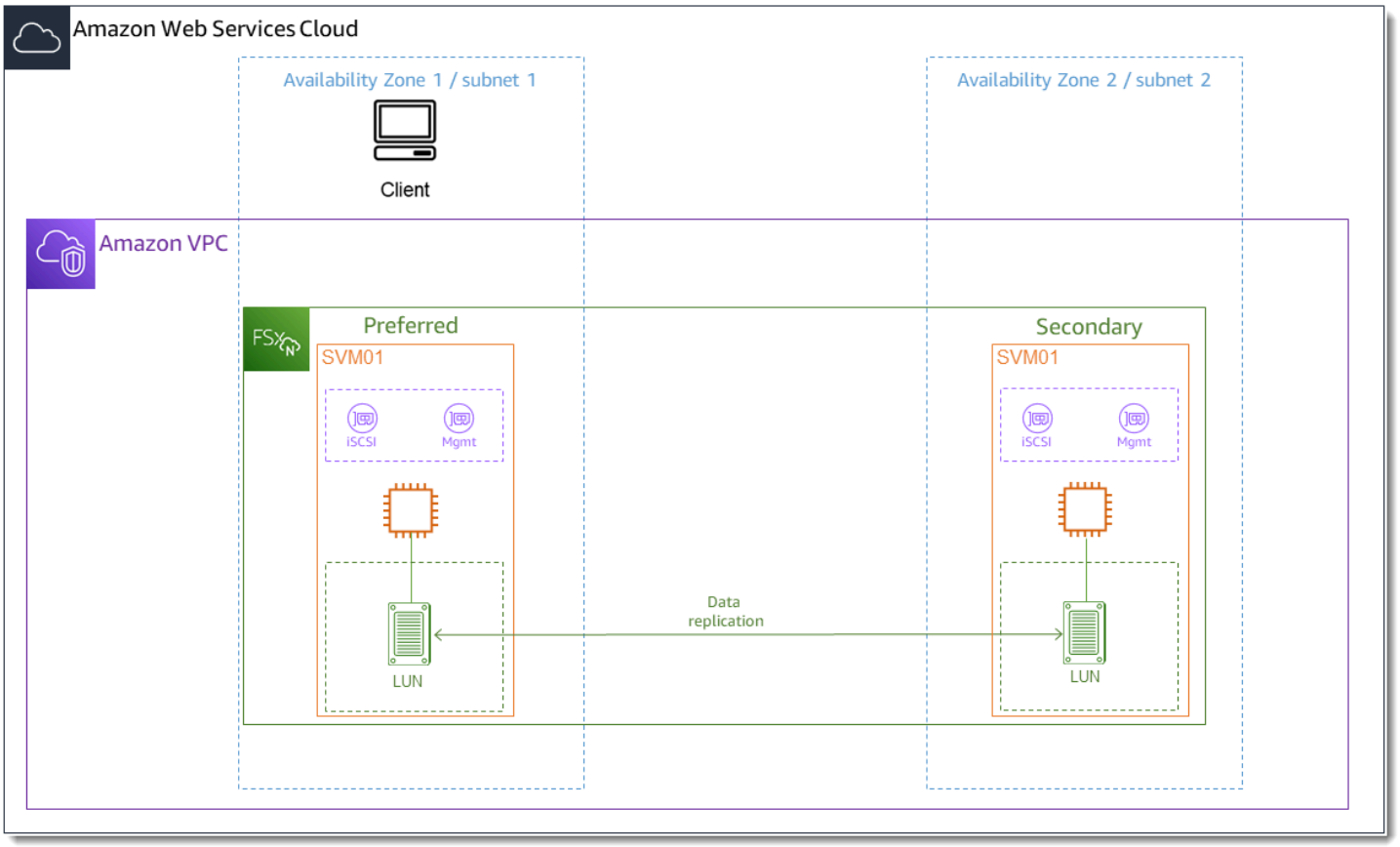
Memasang iSCSI LUN ke klien Windows

Contoh-contoh yang disajikan dalam prosedur ini menggunakan pengaturan berikut:

- ISCSI LUN yang dipasang ke host Windows sudah dibuat. Untuk informasi selengkapnya, lihat Membuat iSCSI LUN.
- Host Microsoft Windows yang memasang iSCSI LUN adalah instans Amazon EC2 yang menjalankan Microsoft Windows Server 2019 Amazon Machine Image (AMI). Ini memiliki grup keamanan VPC yang dikonfigurasi untuk memungkinkan lalu lintas masuk dan keluar seperti yang dijelaskan dalam. Kontrol Akses Sistem File dengan Amazon VPC

  Anda mungkin menggunakan Microsoft Windows AMI yang berbeda dalam pengaturan Anda.
- Klien dan sistem file terletak di VPC yang sama dan. Akun AWS Jika klien berada di VPC lain, Anda dapat menggunakan VPC peering atau AWS Transit Gateway untuk memberikan VPC lain akses ke endpoint iSCSI. Untuk informasi selengkapnya, lihat Mengakses data dari luar VPC penyebaran.

Sebaiknya instans EC2 berada di zona ketersediaan yang sama dengan subnet pilihan sistem file Anda, seperti yang ditunjukkan pada grafik berikut.



Topik

- Konfigurasikan iSCSI pada klien Windows
- Konfigurasikan iSCSI pada fsX untuk sistem file ONTAP
- Pasang iSCSI LUN pada klien Windows
- Memvalidasi konfigurasi iSCSI Anda

Konfigurasikan iSCSI pada klien Windows

1. Gunakan Windows Remote Desktop untuk terhubung ke klien Windows tempat Anda ingin memasang iSCSI LUN. Untuk informasi selengkapnya, lihat Connect ke instans Windows menggunakan RDP di Panduan Pengguna Amazon Elastic Compute Cloud.

2. Buka Windows PowerShell sebagai Administrator. Gunakan perintah berikut untuk mengaktifkan iSCSI pada instance Windows Anda dan konfigurasikan layanan iSCSI untuk memulai secara otomatis.

```
PS C:\> Start-Service MSiSCSI
PS C:\> Set-Service -Name msiscsi -StartupType Automatic
```

3. Ambil nama inisiator instance Windows Anda. Anda akan menggunakan nilai ini dalam mengonfigurasi iSCSI pada fsX Anda untuk sistem file ONTAP menggunakan CLI ONTAP. NetApp

```
PS C:\> (Get-InitiatorPort).NodeAddress
```

Sistem merespons dengan port inisiator:

```
iqn.1991-05.com.microsoft:ec2amaz-abc123d
```

4. Untuk mengaktifkan klien Anda untuk secara otomatis failover antara server file Anda, Anda perlu menginstal `Multipath-IO` (MPIO) pada instance Windows Anda. Gunakan perintah berikut ini.

```
PS C:\> Install-WindowsFeature Multipath-IO
```

5. Mulai ulang instance Windows Anda setelah `Multipath-IO` penginstalan selesai. Biarkan instance Windows Anda tetap terbuka untuk melakukan langkah-langkah untuk memasang iSCSI LUN di bagian berikut.

Konfigurasikan iSCSI pada fsX untuk sistem file ONTAP

1. Connect ke NetApp ONTAP CLI pada fsX untuk sistem file ONTAP tempat Anda membuat iSCSI LUN menggunakan perintah berikut. Untuk informasi selengkapnya, lihat Menggunakan CLI NetApp ONTAP.

```
~$ ssh fsxadmin@your_management_endpoint_ip
```

2. Menggunakan lun igroup createCLI NetApp ONTAP, buat grup inisiator, atau. `igroup` Grup inisiator memetakan ke iSCSI LUN dan mengontrol inisiator (klien) mana yang memiliki akses

ke LUNs. Ganti `host_initiator_name` dengan nama inisiator dari host Windows Anda yang Anda ambil dalam prosedur sebelumnya.

```
::> lun igroup create -vserver svm_name -igroup igroup_name -
initiator host_initiator_name -protocol iscsi -ostype windows
```

Jika Anda ingin membuat LUN yang dipetakan ke ini `igroup` tersedia untuk beberapa host, Anda dapat menentukan beberapa nama inisiator yang dipisahkan koma. Untuk informasi selengkapnya, lihat `lun igroup create`di Pusat Dokumentasi NetApp ONTAP.

3. Konfirmasikan telah berhasil `igroup` dibuat menggunakan perintah berikut:

```
::> lun igroup show
```

Sistem merespons dengan output berikut:

```
Vserver    Igroup        Protocol OS Type  Initiators
---------  ------------  -------- -------- ------------------------------------
svm_name   igroup_name   iscsi    windows  iqn.1994-05.com.windows:abcdef12345
```

Dengan yang `igroup` dibuat, Anda siap untuk membuat LUNs dan memetakannya ke. `igroup`

4. Langkah ini mengasumsikan bahwa Anda telah membuat iSCSI LUN. Jika belum, lihat step-by-step instruksi Membuat iSCSI LUN untuk melakukannya.

Buat pemetaan LUN dari LUN ke yang baru. `igroup`

```
::> lun mapping create -vserver svm_name -path /vol/vol_name/lun_name -
igroup igroup_name -lun-id lun_id
```

5. Konfirmasikan bahwa LUN dibuat, online, dan dipetakan dengan perintah berikut:

```
::> lun show -path /vol/vol_name/lun_name
Vserver     Path                            State   Mapped   Type     Size
---------   ------------------------------- ------- -------- -------- --------
svm_name    /vol/vol_name/lun_name          online  mapped   windows  10GB
```

Anda sekarang siap untuk menambahkan target iSCSI pada instance Windows Anda.

6. Ambil alamat IP `iscsi_1` dan `iscsi_2` antarmuka untuk SVM Anda menggunakan perintah berikut:

```
::> network interface show -vserver svm_name
```

```
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
svm_name
            iscsi_1    up/up      172.31.0.143/20    FSxId0123456789abcdef8-01
                                                                   e0e     true
            iscsi_2    up/up      172.31.21.81/20    FSxId0123456789abcdef8-02
                                                                   e0e     true
            nfs_smb_management_1
                       up/up      198.19.250.177/20  FSxId0123456789abcdef8-01
                                                                   e0e     true
3 entries were displayed.
```

Dalam contoh ini, alamat IP `iscsi_1` adalah `172.31.0.143` dan `iscsi_2` is`172.31.21.81`.

Pasang iSCSI LUN pada klien Windows

1. Pada instance Windows Anda, buka PowerShell terminal sebagai Administrator.
2. Anda akan membuat `.ps1` skrip yang melakukan hal berikut:

   - Terhubung ke setiap antarmuka iSCSI sistem file Anda.
   - Menambahkan dan mengkonfigurasi MPIO untuk iSCSI.
   - Menetapkan 8 sesi untuk setiap koneksi iSCSI, yang memungkinkan klien untuk mendorong hingga 40 Gb/s (5.000 MB/s) throughput agregat ke iSCSI LUN. Memiliki 8 sesi memastikan satu klien dapat mendorong kapasitas throughput 4.000 MB/s penuh untuk FSx tingkat tertinggi untuk kapasitas throughput ONTAP. Anda dapat secara opsional mengubah jumlah sesi ke jumlah sesi yang lebih tinggi atau lebih rendah (setiap sesi menyediakan throughput hingga 625 MB/s) dengan memodifikasi skrip for-loop dalam langkah dari ke batas atas lainnya. `#Establish iSCSI connection` `1..8` Untuk informasi selengkapnya, lihat Bandwidth jaringan instans Amazon EC2 di Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Windows.

   Salin kumpulan perintah berikut ke dalam file untuk membuat `.psl` skrip.

   - Ganti `iscsi_1` dan `iscsi_2` dengan alamat IP yang Anda ambil pada langkah sebelumnya.

- Ganti `ec2_ip` dengan alamat IP instance Windows Anda.

```
#iSCSI IP addresses for Preferred and Standby subnets
$TargetPortalAddresses = @("iscsi_1","iscsi_2")

#iSCSI Initator IP Address (Local node IP address)
$LocaliSCSIAddress = "ec2_ip"

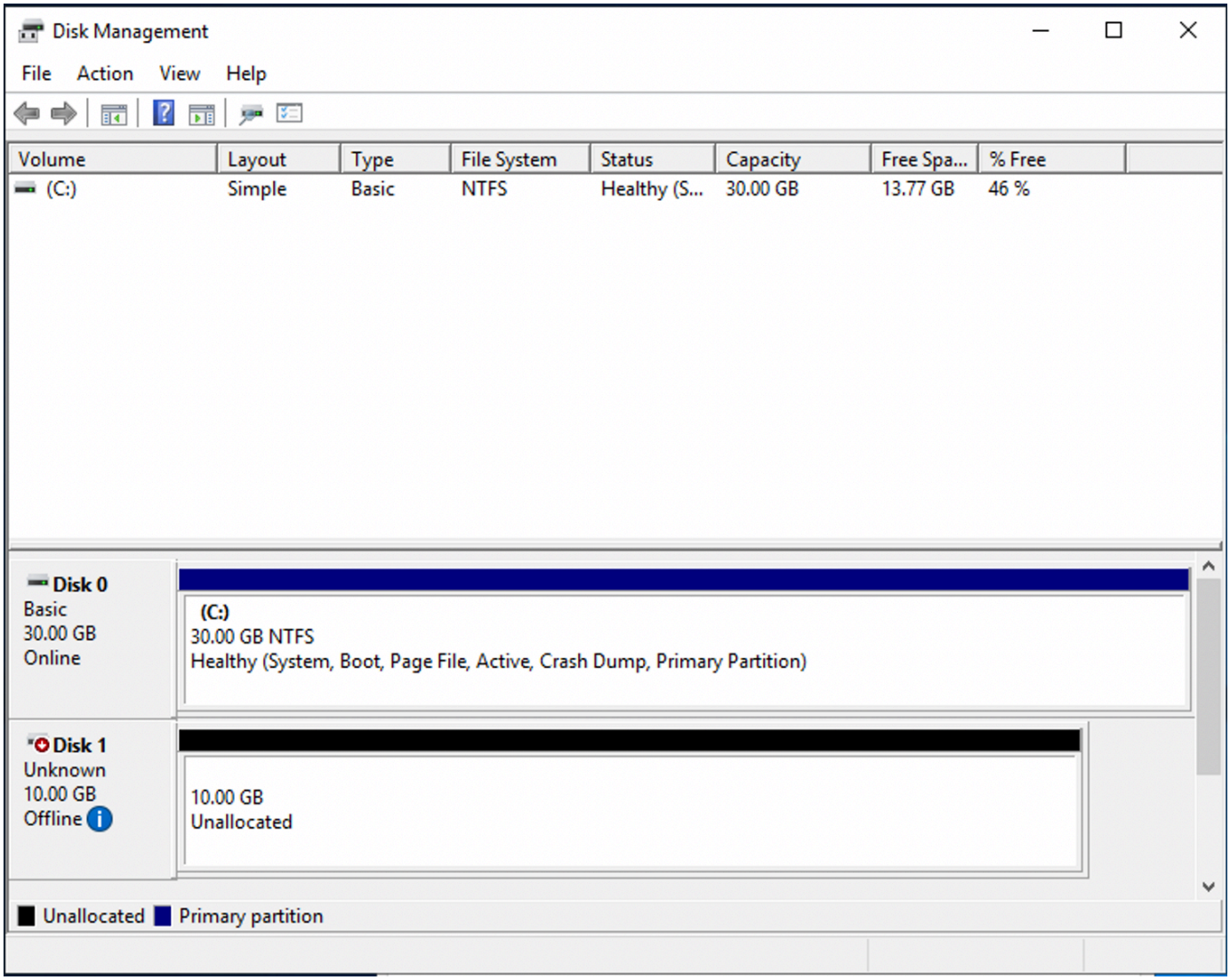
#Connect to FSx for NetApp ONTAP file system
Foreach ($TargetPortalAddress in $TargetPortalAddresses) {
New-IscsiTargetPortal -TargetPortalAddress $TargetPortalAddress -
TargetPortalPortNumber 3260 -InitiatorPortalAddress $LocaliSCSIAddress
}

#Add MPIO support for iSCSI
New-MSDSMSupportedHW -VendorId MSFT2005 -ProductId iSCSIBusType_0x9

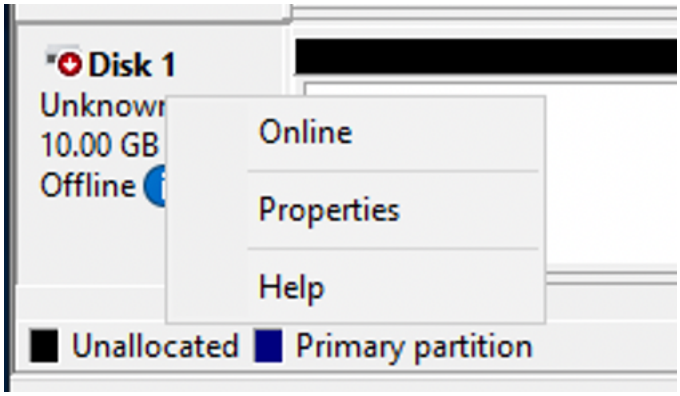
#Establish iSCSI connection
1..8 | %{Foreach($TargetPortalAddress in $TargetPortalAddresses)
{Get-IscsiTarget | Connect-IscsiTarget -IsMultipathEnabled $true -
TargetPortalAddress $TargetPortalAddress -InitiatorPortalAddress $LocaliSCSIAddress
 -IsPersistent $true}}

#Set the MPIO Policy to Round Robin
Set-MSDSMGlobalDefaultLoadBalancePolicy -Policy RR
```

3. Luncurkan aplikasi Windows Disk Management. Buka kotak dialog Windows Run, dan masukkan `diskmgmt.msc` dan tekan Enter. Aplikasi Manajemen Disk terbuka.



4. Temukan disk yang tidak terisi Ini adalah iSCSI LUN. Dalam contoh, Disk 1 adalah disk iSCSI. Ini offline.



Bawa volume online dengan menempatkan kursor di atas Disk 1 dan klik kanan lalu pilih Online.

> **Note**
>
> Anda dapat mengubah kebijakan jaringan area penyimpanan (SAN) sehingga volume baru secara otomatis dibawa online. Untuk informasi selengkapnya, lihat kebijakan SAN di Referensi Perintah Microsoft Windows Server.

5. Untuk menginisialisasi disk, letakkan kursor di atas Disk 1 klik kanan, dan pilih Inisialisasi. Dialog Inisialisasi muncul. Pilih OK inisialisasi disk.
6. Format disk seperti biasanya. Setelah pemformatan selesai, drive iSCSI muncul sebagai drive yang dapat digunakan pada klien Windows.

Memvalidasi konfigurasi iSCSI Anda

Kami telah menyediakan skrip untuk memeriksa apakah pengaturan iSCSI Anda dikonfigurasi dengan benar. Skrip memeriksa parameter seperti jumlah sesi, distribusi node, dan status Multipath I/O (MPIO). Tugas berikut menjelaskan cara menginstal dan menggunakan skrip.

Untuk memvalidasi konfigurasi iSCSI Anda

1. Buka PowerShell jendela Windows.
2. Unduh skrip menggunakan perintah berikut.

```
PS C:\> Invoke-WebRequest "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/
samples/CheckiSCSI.zip" -OutFile "CheckiSCSI.zip"
```

3. Perluas file zip menggunakan perintah berikut.

```
PS C:\> Expand-Archive -Path ".\CheckiSCSI.zip" -DestinationPath "./"
```

4. Jalankan skrip menggunakan perintah berikut.

```
PS C:\> ./CheckiSCSI.ps1
```

5. Tinjau output untuk memahami status konfigurasi Anda saat ini. Contoh berikut menunjukkan konfigurasi iSCSI yang sukses.

```
PS C:\> ./CheckiSCSI.ps1
```

```
This script checks the iSCSI configuration on the local instance.
It will provide information about the number of connected sessions, connected file
 servers, and MPIO status.

MPIO is installed on this server.

Initiator: 'iqn.1991-05.com.microsoft:ec2amaz-d2cebnb'
to Target: 'iqn.1992-08.com.netapp:sn.13266b10e61411ee8bc0c76ad263d613:vs.3'
has 16 total sessions (16 active, 0 non-active)
spread across 2 node(s).
MPIO: Yes
```

Menggunakan fsX untuk ONTAP dengan layanan lain AWS

Selain Amazon EC2, Anda dapat menggunakan AWS layanan lain dengan volume Anda untuk mengakses data Anda.

Topik

- Menggunakan Amazon WorkSpaces dengan FSx untuk ONTAP
- Menggunakan Amazon Elastic Container Service dengan FSx untuk ONTAP
- Menggunakan VMware Cloud dengan FSx untuk ONTAP

Menggunakan Amazon WorkSpaces dengan FSx untuk ONTAP

FSx untuk ONTAP dapat digunakan dengan Amazon WorkSpaces untuk menyediakan penyimpanan terlampir jaringan bersama (NAS) atau untuk menyimpan profil roaming untuk akun Amazon. WorkSpaces Setelah menghubungkan ke berbagi file SMB dengan sebuah WorkSpaces instance, pengguna dapat membuat dan mengedit file pada berbagi file.

Prosedur berikut menunjukkan cara menggunakan Amazon FSx dengan Amazon WorkSpaces untuk memberikan profil roaming dan akses folder rumah pengalaman yang konsisten dan untuk menyediakan folder tim bersama untuk pengguna Windows dan Linux. WorkSpaces Jika Anda baru mengenal Amazon WorkSpaces, Anda dapat membuat WorkSpaces lingkungan Amazon pertama Anda dengan petunjuk di Memulai dengan Pengaturan WorkSpaces Cepat di Panduan WorkSpaces Administrasi Amazon.

Topik

Berikan dukungan Profil Roaming

Anda dapat menggunakan Amazon FSx untuk memberikan dukungan Profil Roaming kepada pengguna di organisasi Anda. Seorang pengguna akan memiliki izin untuk hanya mengakses Profil Roaming mereka. Folder akan terhubung secara otomatis menggunakan Kebijakan Grup Direktori Aktif. Dengan Profil Roaming, data pengguna dan pengaturan desktop disimpan saat mereka keluar dari berbagi file Amazon FSx yang memungkinkan dokumen dan pengaturan untuk dibagikan di antara WorkSpaces instans yang berbeda, dan secara otomatis dicadangkan menggunakan cadangan otomatis harian Amazon FSx.

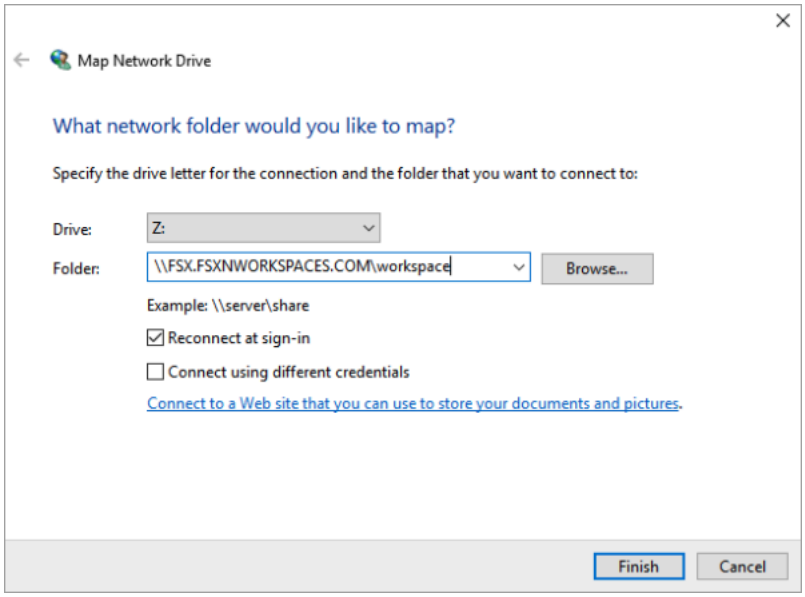
Langkah 1: Buat lokasi folder profil untuk pengguna domain menggunakan Amazon FSx

1. Buat fsX untuk sistem file ONTAP menggunakan konsol Amazon FSx. Untuk informasi selengkapnya, lihat Untuk membuat sistem file (konsol).

   > **Important**
   >
   > Setiap fsX untuk sistem file ONTAP memiliki rentang alamat IP titik akhir dari mana titik akhir yang terkait dengan sistem file dibuat. Untuk sistem file multi-AZ, FSx untuk ONTAP memilih rentang alamat IP default yang tidak digunakan dari 198.19.0.0/16 sebagai rentang alamat IP titik akhir. Rentang alamat IP ini juga digunakan oleh WorkSpaces untuk rentang lalu lintas manajemen, seperti yang dijelaskan dalam alamat IP dan persyaratan port untuk WorkSpaces dalam Panduan WorkSpaces Administrasi Amazon. Akibatnya, untuk mengakses Multi-AZ FSx untuk sistem file ONTAP WorkSpaces dari, Anda harus memilih rentang alamat IP titik akhir yang tidak tumpang tindih dengan 198.19.0.0/16.

2. Jika Anda tidak memiliki mesin virtual penyimpanan (SVM) yang bergabung dengan Active Directory, buat sekarang. Misalnya, Anda dapat menyediakan SVM bernama `fsx` dan mengatur gaya keamanan keNTFS. Untuk informasi selengkapnya, lihat Untuk membuat penyimpanan mesin virtual (konsol).

3. Buat volume untuk SVM Anda. Misalnya, Anda dapat membuat volume bernama `fsx-vol` yang mewarisi gaya keamanan volume root SVM Anda. Untuk informasi selengkapnya, lihat Untuk membuat FlexVol volume (konsol).
4. Buat berbagi SMB pada volume Anda. Misalnya, Anda dapat membuat share yang dipanggil `workspace` pada volume Anda bernama`fsx-vol`, di mana Anda membuat folder bernama`profiles`. Untuk informasi selengkapnya, lihat Mengelola saham SMB.
5. Akses Amazon FSx SVM Anda dari instans Amazon EC2 yang menjalankan Windows Server atau dari file. WorkSpace Untuk informasi selengkapnya, lihat Mengakses data.
6. Anda memetakan bagian Anda ke `Z:\` WorkSpaces instans Windows Anda:



Langkah 2: Tautkan FSx untuk berbagi file ONTAP ke Akun Pengguna

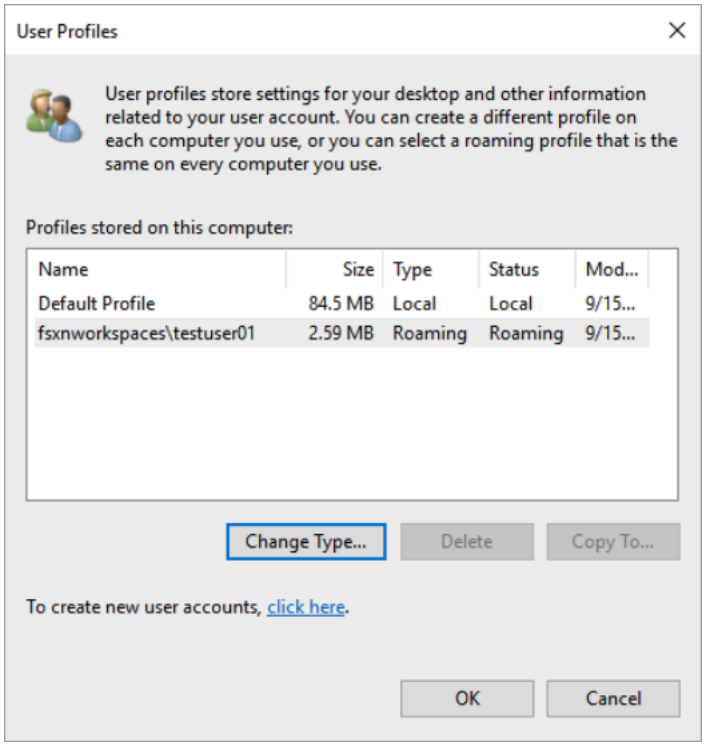
1. Pada pengguna pengujian Anda WorkSpace, pilih Windows > System > Advanced System Settings.
2. Di System Properties, pilih tab Advanced dan tekan tombol Pengaturan di bagian Profil Pengguna. Pengguna yang masuk akan memiliki tipe profil. `Local`
3. Keluar dari pengguna uji dari file WorkSpace.
4. Atur pengguna uji agar profil roaming terletak di sistem file Amazon FSx Anda. Di administrator Anda WorkSpaces, buka PowerShell konsol dan gunakan perintah yang mirip dengan contoh berikut (yang menggunakan `profiles` folder yang sebelumnya Anda buat di Langkah 1):

```
Set-ADUser username -ProfilePath \\filesystem-dns-
name\sharename\foldername\username
```

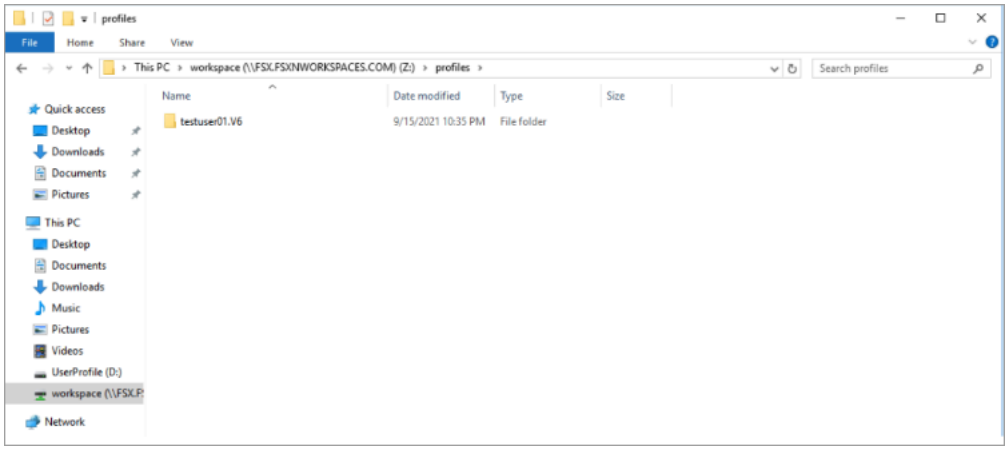
Misalnya:

```
Set-ADUser testuser01 -ProfilePath \\fsx.fsxnworkspaces.com\workspace\profiles
\testuser01
```

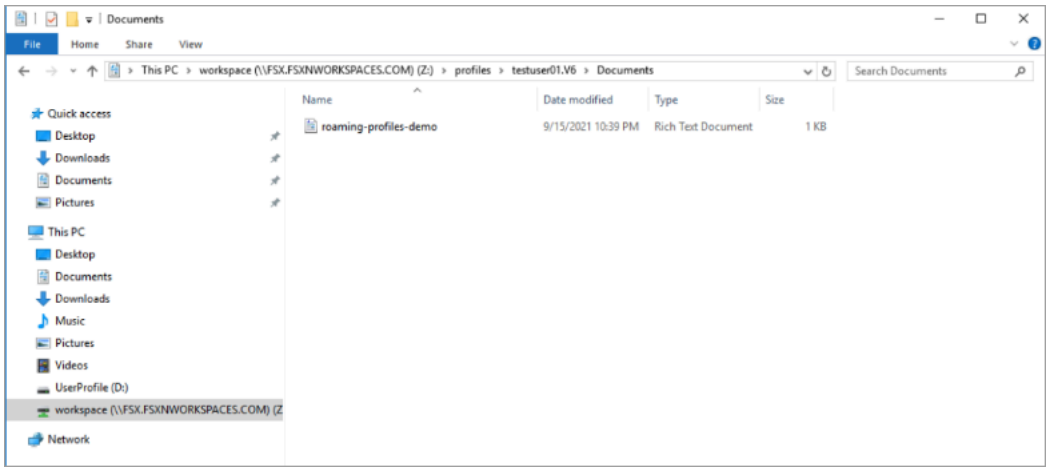
5. Masuk ke pengguna uji WorkSpace.
6. Di System Properties, pilih tab Advanced dan tekan tombol Pengaturan di bagian Profil Pengguna. Pengguna yang masuk akan memiliki tipe profil. `Roaming`



7. Jelajahi folder bersama FSx untuk ONTAP. Di `profiles` folder, Anda akan melihat folder untuk pengguna.



8. Buat dokumen di `Documents` folder pengguna uji
9. Keluar dari pengguna uji dari mereka WorkSpace.
10. Jika Anda masuk kembali sebagai pengguna uji dan menjelajah ke toko profil mereka, Anda akan melihat dokumen yang Anda buat.



Menyediakan folder bersama untuk mengakses file umum

Anda dapat menggunakan Amazon FSx untuk menyediakan sebuah folder bersama untuk pengguna di organisasi Anda. Folder bersama dapat digunakan untuk menyimpan file yang digunakan oleh komunitas pengguna Anda, seperti file demo, contoh kode, dan instruksi manual yang dibutuhkan oleh semua pengguna. Biasanya, Anda memiliki drive yang dipetakan untuk folder bersama; Namun karena drive yang dipetakan menggunakan huruf, ada batasan jumlah saham yang dapat Anda miliki. Prosedur ini membuat folder bersama Amazon FSx yang tersedia tanpa huruf drive, memberi Anda fleksibilitas yang lebih besar dalam menetapkan pembagian ke tim.

Untuk me-mount folder bersama untuk akses lintas platform dari Linux dan Windows WorkSpaces

1. Dari Taskbar, pilih Places > Connect to Server.

   a. Untuk Server, masukkan *`file-system-dns-name`*.

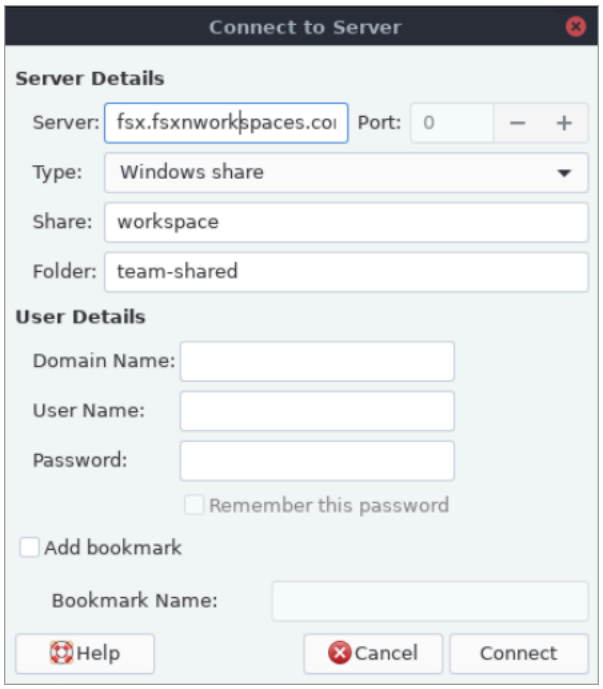
   b. Atur Type ke`Windows share`.

   c. Setel Bagikan ke nama berbagi SMB, sepertiworkspace.

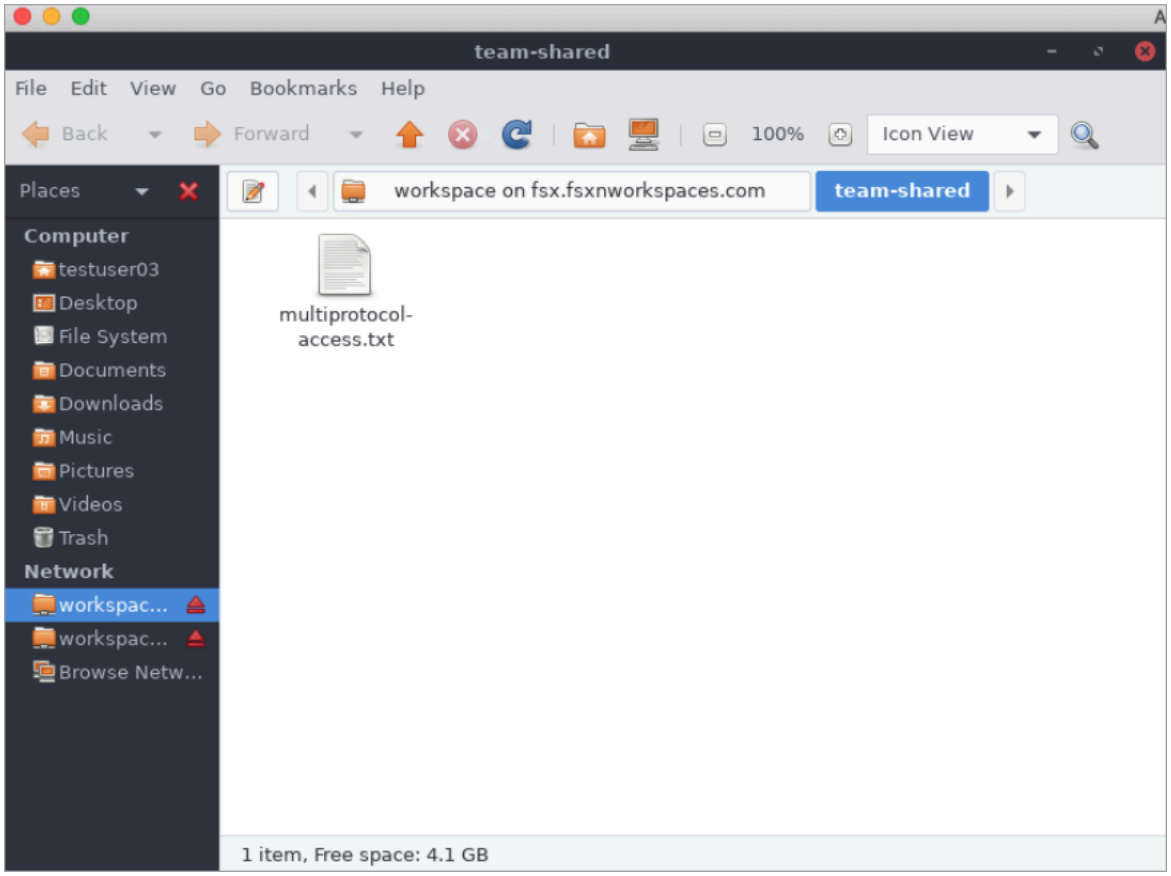
   d. Anda dapat meninggalkan Folder sebagai / atau mengaturnya ke folder, seperti folder bernamateam-shared.

   e. Untuk Linux WorkSpace, Anda tidak perlu memasukkan detail pengguna jika Linux Anda WorkSpace berada di domain yang sama dengan berbagi Amazon FSx.

   f. Pilih Hubungkan.



2. Setelah koneksi dibuat, Anda dapat melihat folder bersama (dinamai `team-shared` dalam contoh ini) di berbagi SMB bernamaworkspace.



Menggunakan Amazon Elastic Container Service dengan FSx untuk ONTAP

Anda dapat mengakses Amazon FSx untuk sistem file NetApp ONTAP dari wadah Amazon Elastic Container Service (Amazon ECS) Docker Container Service (Amazon ECS) pada instans Amazon EC2 Linux atau Windows.

Memasang pada wadah Amazon ECS Linux

1. Buat cluster ECS menggunakan template cluster EC2 Linux + Networking untuk wadah Linux Anda. Untuk informasi selengkapnya, lihat Membuat klaster di Panduan Pengembang Layanan Amazon Elastic Container.
2. Buat direktori pada instans EC2 untuk memasang volume SVM sebagai berikut:

```
sudo mkdir /fsxontap
```

3. Pasang FSx Anda untuk volume ONTAP pada instans Linux EC2 dengan menggunakan skrip data pengguna selama peluncuran instance, atau dengan menjalankan perintah berikut:

```
sudo mount -t nfs svm-ip-address:/vol1 /fsxontap
```

4. Pasang volume menggunakan perintah berikut:

```
sudo mount -t nfs -o nfsvers=NFS_version svm-dns-name:/volume-junction-path /
fsxontap
```

Contoh berikut menggunakan nilai sampel.

```
sudo mount -t nfs -o nfsvers=4.1
 svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /
fsxontap
```

Anda juga dapat menggunakan SVM alamat IP SVM alih-alih nama DNS.

```
sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
```

5. Saat membuat definisi tugas Amazon ECS, tambahkan properti berikut `volumes` dan `mountPoints` container dalam definisi container JSON. Ganti `sourcePath` dengan titik pemasangan dan direktori di FSx Anda untuk sistem file ONTAP.

```
{
    "volumes": [
        {
            "name": "ontap-volume",
            "host": {
                "sourcePath": "mountpoint"
            }
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
    .
    .
```

```
    .
}
```

Memasang pada wadah Amazon ECS Windows

1. Buat cluster ECS menggunakan template cluster EC2 Windows+Networking untuk wadah Windows Anda. Untuk informasi selengkapnya, lihat Membuat klaster di Panduan Pengembang Layanan Amazon Elastic Container.
2. Tambahkan instance Windows EC2 yang bergabung dengan domain ke cluster ECS Windows dan petakan berbagi SMB.

   Luncurkan instans EC2 Windows yang dioptimalkan ECS yang digabungkan ke domain Active Directory Anda dan inisialisasi agen ECS dengan menjalankan perintah berikut.

   ```
   PS C:\Users\user> Initialize-ECSAgent -Cluster windows-fsx-cluster -
   EnableTaskIAMRole
   ```

   Anda juga dapat meneruskan informasi dalam skrip ke bidang teks data pengguna sebagai berikut.

   ```
   <powershell>
   Initialize-ECSAgent -Cluster windows-fsx-cluster -EnableTaskIAMRole
   </powershell>
   ```

3. Buat pemetaan global SMB pada instans EC2 sehingga Anda dapat memetakan berbagi SMB Anda ke drive. Ganti nilai di bawah netbios atau nama DNS untuk sistem file FSx Anda dan bagikan nama. Volume NFS vol1 yang dipasang pada instans Linux EC2 dikonfigurasi sebagai fsxontap berbagi CIFS pada sistem file FSx.

   ```
   vserver cifs share show -vserver svm08 -share-name fsxontap


                                   Vserver: svm08
                                     Share: fsxontap
                   CIFS Server NetBIOS Name: FSX0NTAPDEMO
                                     Path: /vol1
                            Share Properties: oplocks
                                              browsable
                                              changenotify
   ```

```
                                            show-previous-versions
                          Symlink Properties: symlinks
                     File Mode Creation Mask: -
                Directory Mode Creation Mask: -
                               Share Comment: -
                                   Share ACL: Everyone / Full Control
            File Attribute Cache Lifetime: -
                                 Volume Name: vol1
                               Offline Files: manual
            Vscan File-Operations Profile: standard
          Maximum Tree Connections on Share: 4294967295
                 UNIX Group for File Create: -
```

4. Buat pemetaan global SMB pada instans EC2 menggunakan perintah berikut:

```
New-SmbGlobalMapping -RemotePath \\fsxontapdemo.fsxontap.com\fsxontap -LocalPath Z:
```

5. Saat membuat definisi tugas Amazon ECS, tambahkan properti berikut `volumes` dan `mountPoints` container dalam definisi container JSON. Ganti `sourcePath` dengan titik pemasangan dan direktori di FSx Anda untuk sistem file ONTAP.

```
{
    "volumes": [
        {
            "name": "ontap-volume",
            "host": {
                "sourcePath": "mountpoint"
            }
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
    .
    .
    .
}
```

Menggunakan VMware Cloud dengan FSx untuk ONTAP

Anda dapat menggunakan FSx untuk ONTAP sebagai datastore eksternal untuk VMware Cloud pada AWS Pusat Data yang Ditetapkan Perangkat Lunak (SDDC). Untuk informasi selengkapnya, lihat Mengonfigurasi Amazon FSx untuk NetApp ONTAP sebagai Penyimpanan Eksternal dan VMware Cloud dengan AWS Amazon FSx untuk Panduan Penerapan ONTAP. NetApp

Ketersediaan dan daya tahan

Amazon FSx untuk NetApp ONTAP menggunakan dua jenis penyebaran, Single-AZ dan Multi-AZ, yang menawarkan berbagai tingkat ketersediaan dan daya tahan. Topik ini menjelaskan fitur ketersediaan dan daya tahan dari setiap jenis penerapan untuk membantu Anda memilih salah satu yang tepat untuk beban kerja Anda. Untuk informasi tentang ketersediaan layanan SLA (Perjanjian Tingkat Layanan), lihat Perjanjian Tingkat Layanan Amazon FSx.

Topik

Memilih jenis penyebaran sistem file

Fitur ketersediaan dan daya tahan tipe penyebaran sistem file Single-AZ dan Multi-AZ dijelaskan di bagian berikut.

Jenis penyebaran AZ tunggal

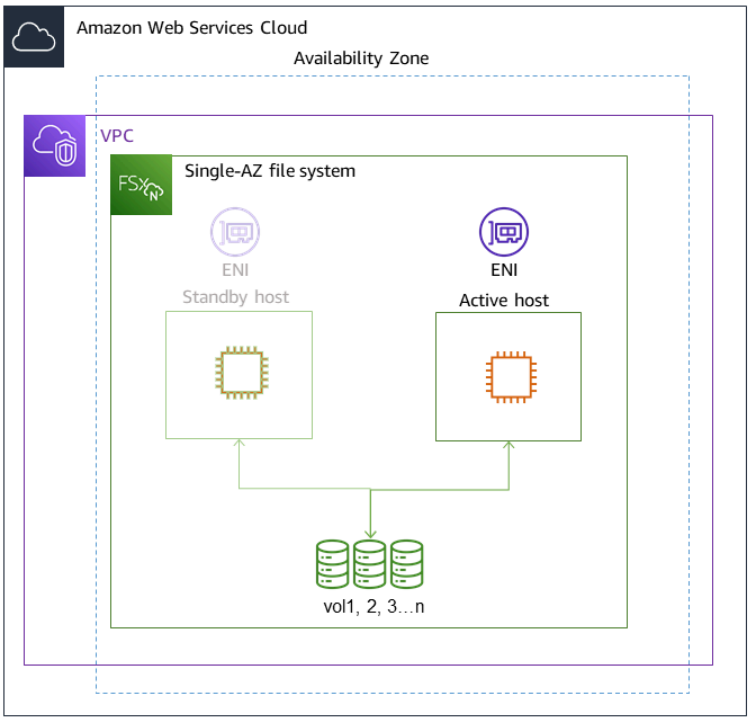
Saat Anda membuat sistem file Single-AZ, Amazon FSx secara otomatis menyediakan satu hingga dua belas pasang server file dalam konfigurasi siaga aktif, dengan server file aktif dan siaga di setiap pasangan yang terletak di domain kesalahan terpisah dalam satu Availability Zone di. Wilayah AWS Selama pemeliharaan sistem file yang direncanakan atau gangguan layanan yang tidak direncanakan dari server file aktif apa pun, Amazon FSx secara otomatis dan independen gagal atas pasangan ketersediaan tinggi (HA) ke server file siaga, biasanya dalam beberapa detik. Selama failover, Anda terus memiliki akses ke data Anda tanpa intervensi manual.

Untuk memastikan ketersediaan yang tinggi, Amazon FSx terus memantau kegagalan perangkat keras, dan secara otomatis mengganti komponen infrastruktur jika terjadi kegagalan. Untuk mencapai daya tahan tinggi, Amazon FSx secara otomatis mereplikasi data Anda dalam Availability Zone untuk melindunginya dari kegagalan komponen. Selain itu, Anda memiliki opsi untuk mengonfigurasi pencadangan harian otomatis dari data sistem file Anda. Pencadangan ini disimpan di beberapa Availability Zone untuk memberikan ketahanan Multi-AZ untuk semua data cadangan.

Sistem file single-AZ dirancang untuk kasus penggunaan yang tidak memerlukan model ketahanan data dari sistem file Multi-AZ. Mereka menyediakan solusi yang dioptimalkan biaya untuk kasus

penggunaan seperti lingkungan pengembangan dan pengujian, atau menyimpan salinan sekunder data yang sudah disimpan di tempat atau di tempat lain Wilayah AWS, dengan hanya mereplikasi data dalam satu Availability Zone.

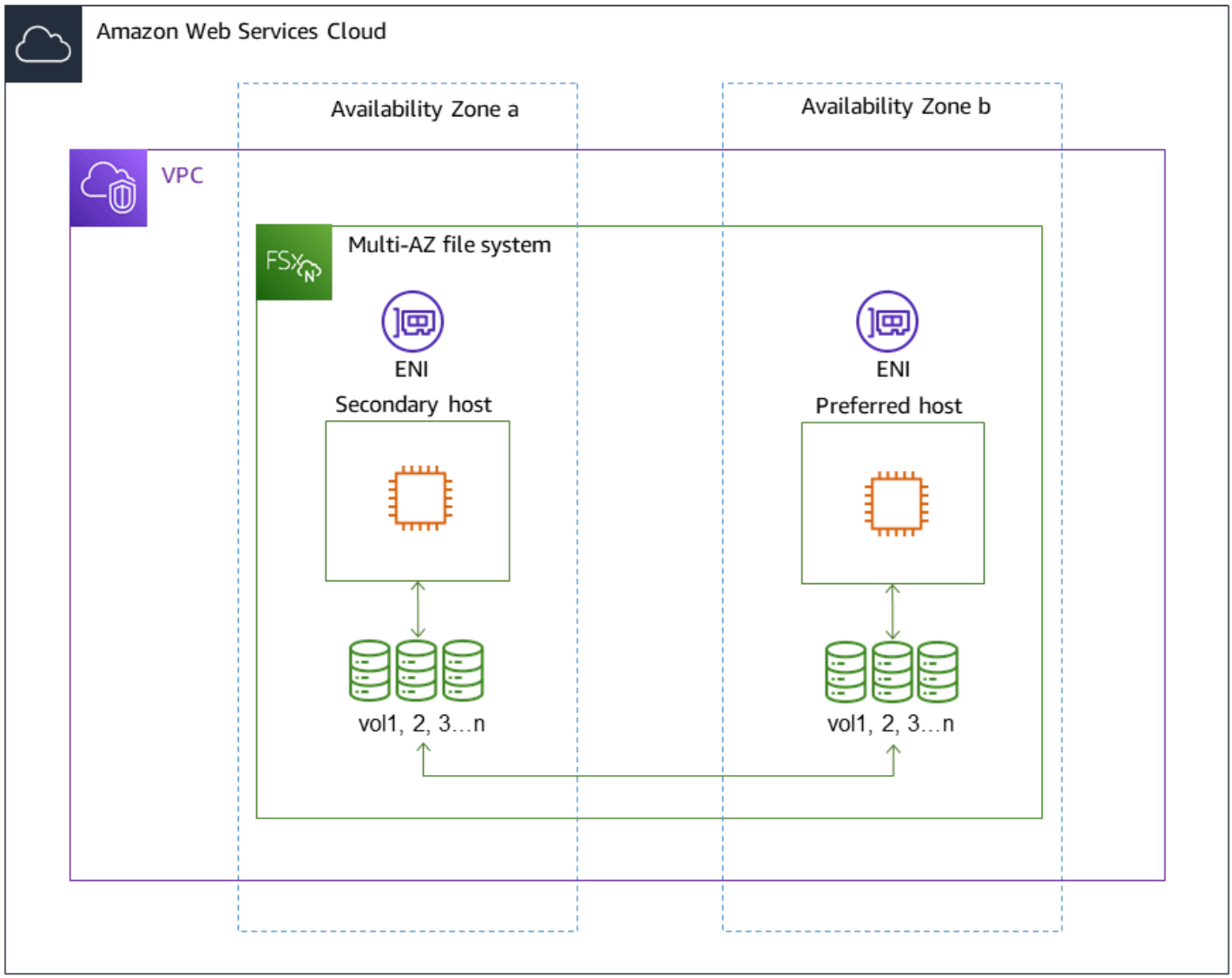
Diagram berikut menggambarkan arsitektur untuk FSx untuk sistem file ONTAP Single-AZ.



Jenis penyebaran multi-AZ

Sistem file Multi-AZ mendukung semua fitur ketersediaan dan daya tahan sistem file Single-AZ. Selain itu, mereka dirancang untuk menyediakan ketersediaan data yang berkelanjutan bahkan ketika Availability Zone tidak tersedia. Penerapan multi-AZ memiliki sepasang HA tunggal server file, server file siaga digunakan di Availability Zone yang berbeda dari server file aktif yang sama. Wilayah AWS Setiap perubahan yang ditulis ke sistem file Anda direplikasi secara sinkron di seluruh Availability Zones ke standby.

Sistem file multi-AZ dirancang untuk kasus penggunaan seperti beban kerja produksi penting bisnis yang memerlukan ketersediaan tinggi untuk data file ONTAP bersama dan membutuhkan penyimpanan dengan replikasi bawaan di seluruh Availability Zone. Diagram berikut menggambarkan arsitektur untuk FSx untuk sistem file Multi-AZ ONTAP.



Proses failover untuk FSx untuk ONTAP

Sistem file single-AZ dan Multi-AZ secara otomatis gagal pada pasangan HA tertentu dari server file pilihan atau aktif ke server file siaga jika salah satu kondisi berikut terjadi:

- Server file pilihan atau aktif menjadi tidak tersedia
- Kapasitas throughput sistem file diubah
- Server file yang disukai atau aktif menjalani pemeliharaan yang direncanakan
- Terjadi pemadaman Zona Ketersediaan (hanya sistem file multi-AZ)

> **Note**
>
> Untuk sistem file scale-out, perilaku failover setiap pasangan HA bersifat independen. Jika server file pilihan untuk satu pasangan HA tidak tersedia, hanya pasangan HA yang akan gagal ke server file siaga.

Ketika gagal dari satu server file ke server lain, server file aktif baru secara otomatis mulai melayani semua permintaan baca dan tulis sistem file ke pasangan HA tersebut. Untuk sistem file multi-AZ, ketika server file pilihan sepenuhnya pulih dan tersedia, Amazon FSx secara otomatis gagal kembali ke sana, dengan failback biasanya selesai dalam waktu kurang dari 60 detik. Untuk sistem file Single-AZ dan Multi-AZ, failover biasanya selesai dalam waktu kurang dari 60 detik dari deteksi kegagalan pada server file aktif hingga promosi server file siaga ke status aktif. Karena alamat IP endpoint yang digunakan klien untuk mengakses data melalui NFS atau SMB tetap sama, failover transparan untuk aplikasi Linux, Windows, dan macOS, yang melanjutkan operasi sistem file tanpa intervensi manual.

Untuk memastikan bahwa failover transparan ke klien yang terhubung ke FSx Anda untuk sistem file ONTAP Single-AZ dan Multi-AZ, lihat. Mengakses data dari dalam AWS

Menguji failover pada sebuah sistem file

Anda dapat menguji failover pada sistem file scale-up Anda dengan memodifikasi kapasitas throughputnya. Saat Anda memodifikasi kapasitas throughput sistem file Anda, Amazon FSx mengalihkan server file sistem file secara serial. Sistem file secara otomatis gagal ke server sekunder sementara Amazon FSx menggantikan server file pilihan terlebih dahulu. Setelah diperbarui, sistem file secara otomatis gagal kembali ke server utama baru dan Amazon FSx menggantikan server file sekunder.

Anda dapat memantau kemajuan permintaan pembaruan kapasitas throughput di konsol Amazon FSx, CLI, dan API. Untuk informasi lebih lanjut tentang memodifikasi kapasitas throughput sistem file Anda dan memantau kemajuan permintaan, lihat Mengelola kapasitas throughput.

Sumber daya jaringan

Bagian ini menjelaskan sumber daya jaringan yang dikonsumsi oleh sistem file Single-AZ dan Multi-AZ.

Subnet

Saat Anda membuat sistem file Single-AZ, Anda menentukan satu subnet untuk sistem file. Subnet yang Anda pilih mendefinisikan Availability Zone tempat sistem file tersebut dibuat. Ketika Anda membuat sebuah sistem file Multi-AZ, Anda menentukan dua subnet, satu untuk server file pilihan, dan satu untuk server file siaga. Dua subnet yang Anda pilih harus berada di Availability Zone yang berbeda dalam hal yang sama Wilayah AWS. Untuk informasi selengkapnya tentang Amazon VPC, lihat Apa itu Amazon VPC? di Panduan Pengguna Amazon Virtual Private Cloud.

> **Note**
>
> Terlepas dari subnet yang Anda tentukan, Anda dapat mengakses sistem file Anda dari subnet apa pun dalam VPC sistem file.

Antarmuka jaringan elastis sistem file

Untuk sistem file Single-AZ, Amazon FSx menyediakan dua antarmuka jaringan elastis (ENI) di subnet yang Anda kaitkan dengan sistem file Anda. Untuk sistem file multi-AZ, Amazon FSx juga menyediakan dua ENI, satu di setiap subnet yang Anda kaitkan dengan sistem file Anda. Klien berkomunikasi dengan sistem file Amazon FSx Anda menggunakan elastic network interface. Antarmuka jaringan dianggap berada dalam lingkup layanan Amazon FSx, meskipun menjadi bagian dari VPC akun Anda. Sistem file multi-AZ menggunakan alamat protokol internet (IP) mengambang sehingga klien yang terhubung dengan mulus bertransisi antara server file pilihan dan siaga selama acara failover.

> **Warning**
>
> - Anda tidak boleh mengubah atau menghapus antarmuka jaringan elastis yang dikaitkan dengan sistem file Anda. Memodifikasi atau menghapus antarmuka jaringan dapat menyebabkan koneksi hilang permanen antara VPC dan sistem file Anda.
> - Antarmuka jaringan elastis yang terkait dengan sistem file Anda akan memiliki rute yang dibuat secara otomatis dan ditambahkan ke tabel rute VPC dan subnet default Anda. Memodifikasi atau menghapus rute ini dapat menyebabkan hilangnya konektivitas sementara atau permanen untuk klien sistem file Anda.

Tabel berikut merangkum sumber daya subnet, elastic network interface, dan IP address untuk masing-masing fsX untuk jenis penyebaran sistem file ONTAP:

	Single-AZ (peningkatan skala)	Single-AZ (scale-out)	Multi-AZ (peningkatan skala)
Jumlah subnet	1	1	2
Jumlah antarmuka jaringan elastis	2	2 per pasangan HA	2
Jumlah alamat IP per ENI	1 + jumlah SVM dalam sistem file	Jumlah pasangan HA+jumlah pasangan HA dikalikan dengan jumlah SVM dalam sistem file	1 + jumlah SVM dalam sistem file
Jumlah rute tabel rute VPC	N/A	N/A	1 + jumlah SVM dalam sistem file

Setelah sistem file atau SVM dibuat, alamat IP-nya tidak berubah sampai sistem file dihapus.

> **Important**
>
> Amazon FSx tidak mendukung akses sistem file dari, atau mengekspos sistem file ke Internet publik. Amazon FSx secara otomatis melepaskan alamat IP Elastic yang merupakan alamat IP publik yang dapat dijangkau dari Internet, yang akan dilampirkan ke antarmuka network elastis sistem file.

Mengelola kapasitas penyimpanan

Amazon FSx untuk NetApp ONTAP menyediakan sejumlah fitur terkait penyimpanan yang dapat Anda gunakan untuk mengelola kapasitas penyimpanan pada sistem file Anda.

Topik

fsX untuk tingkatan penyimpanan ONTAP

Tingkat penyimpanan adalah media penyimpanan fisik untuk Amazon FSx NetApp untuk sistem file ONTAP. FSx untuk ONTAP menawarkan tingkatan penyimpanan berikut:

- Tingkat SSD - Penyimpanan solid-state drive (SSD) berkinerja tinggi yang disediakan pengguna yang dibuat khusus untuk bagian aktif kumpulan data Anda.
- Tingkat kolam kapasitas — Penyimpanan yang sepenuhnya elastis yang secara otomatis menskalakan ke ukuran petabyte, dan dioptimalkan biaya untuk data Anda yang jarang diakses.

FSx untuk volume ONTAP adalah sumber daya virtual yang, mirip dengan folder, tidak mengkonsumsi kapasitas penyimpanan. Data yang Anda simpan—dan yang menghabiskan penyimpanan fisik—hidup di dalam volume. Saat Anda membuat volume, Anda menentukan ukurannya—yang dapat Anda ubah setelah dibuat. FSx untuk volume ONTAP disediakan tipis, dan penyimpanan sistem file tidak dicadangkan sebelumnya. Sebaliknya, SSD dan penyimpanan kolam kapasitas dialokasikan secara dinamis, sesuai kebutuhan. Kebijakan tiering, yang Anda konfigurasikan pada tingkat volume, menentukan apakah dan kapan data yang disimpan dalam transisi tingkat SSD ke tingkat kumpulan kapasitas.

Diagram berikut menggambarkan contoh data yang diletakkan di beberapa FSx untuk volume ONTAP dalam sistem file.

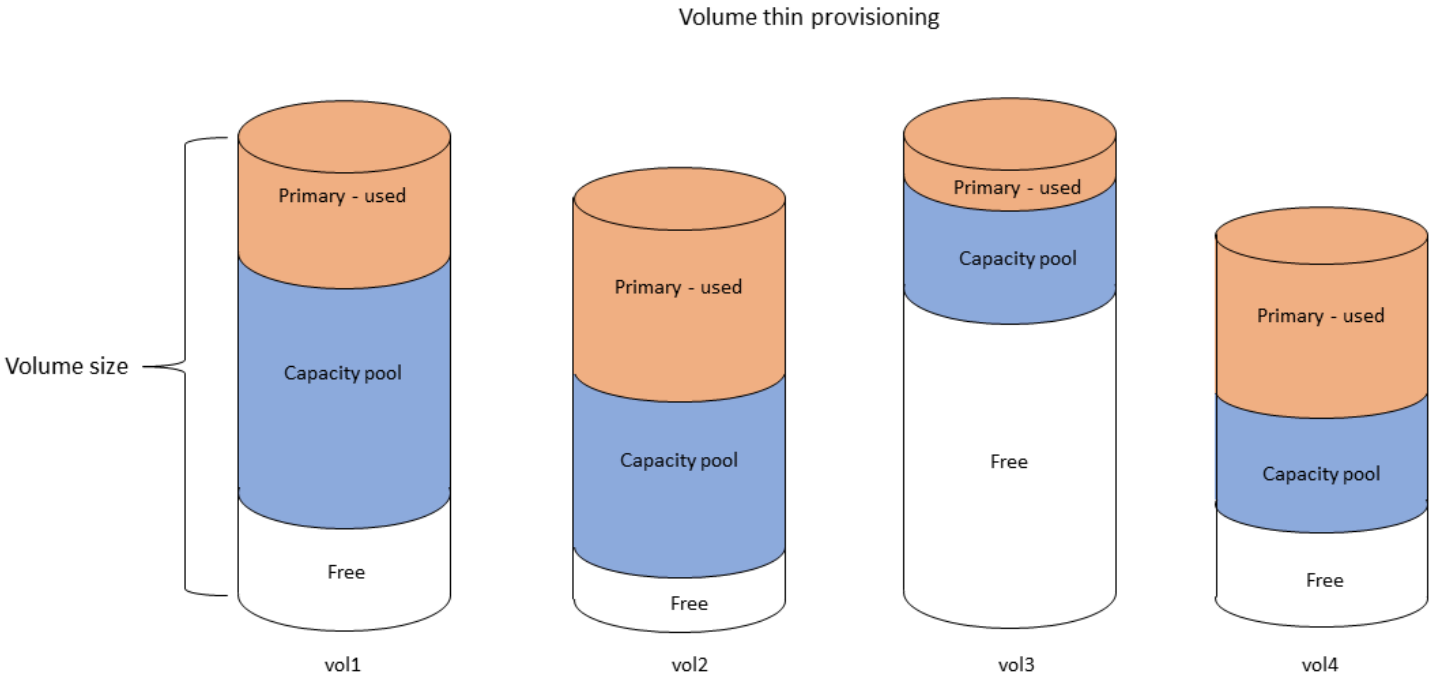
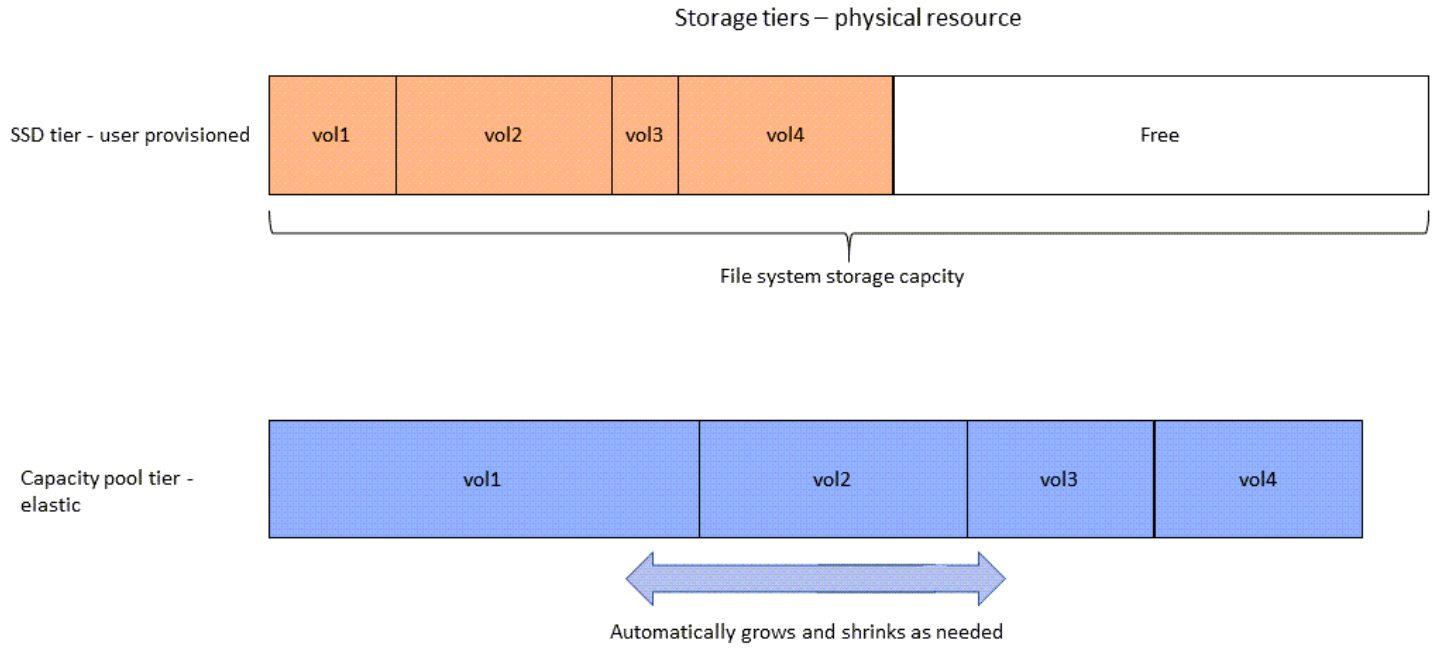


Diagram berikut menggambarkan bagaimana kapasitas penyimpanan fisik sistem file dikonsumsi oleh data dalam empat volume pada diagram sebelumnya.



Anda dapat mengurangi biaya penyimpanan dengan memilih kebijakan tiering yang paling memenuhi persyaratan untuk setiap volume pada sistem file Anda. Untuk informasi selengkapnya, lihat Tingkat data volume.

Memilih jumlah penyimpanan SSD sistem file yang tepat

Saat memilih jumlah kapasitas penyimpanan SSD untuk FSx Anda untuk sistem file ONTAP, Anda perlu mengingat item berikut yang memengaruhi jumlah penyimpanan SSD yang tersedia untuk menyimpan data Anda:

- Kapasitas penyimpanan dicadangkan untuk overhead perangkat lunak NetApp ONTAP.
- Metadata berkas
- Data yang baru ditulis
- File yang ingin Anda simpan di penyimpanan SSD, apakah itu data yang belum mencapai periode pendinginannya, atau data yang baru-baru ini Anda baca yang diambil kembali ke SSD.

Bagaimana penyimpanan SSD digunakan

Penyimpanan SSD sistem file Anda digunakan untuk kombinasi perangkat lunak NetApp ONTAP (overhead), metadata file, dan data Anda.

NetApp Overhead perangkat lunak ONTAP

Seperti sistem file NetApp ONTAP lainnya, hingga 16% dari kapasitas penyimpanan SSD sistem file dicadangkan untuk overhead ONTAP, yang berarti tidak tersedia untuk menyimpan file Anda. Overhead ONTAP dialokasikan sebagai berikut:

- 11% dicadangkan untuk perangkat lunak NetApp ONTAP. Untuk sistem file dengan kapasitas penyimpanan SSD lebih dari 30 tebibytes (TiB), 6% dicadangkan.
- 5% dicadangkan untuk snapshot agregat, yang diperlukan untuk menyinkronkan data antara kedua server file sistem file.

Metadata berkas

Metadata file biasanya mengkonsumsi 3-7% dari kapasitas penyimpanan yang dikonsumsi oleh file. Persentase ini tergantung pada ukuran file rata-rata (ukuran file rata-rata yang lebih kecil membutuhkan lebih banyak metadata), dan jumlah penghematan efisiensi penyimpanan yang dicapai pada file Anda. Perhatikan bahwa metadata file tidak mendapat manfaat dari penghematan efisiensi penyimpanan. Anda dapat menggunakan panduan berikut untuk memperkirakan jumlah penyimpanan SSD yang digunakan untuk metadata pada sistem file Anda.

Ukuran file rata-rata	Ukuran metadata sebagai persentase data file
4 KB	7%
8 KB	3,5%
32 KB atau lebih	1-3%

Saat mengukur jumlah kapasitas penyimpanan SSD yang Anda butuhkan untuk metadata file yang Anda rencanakan untuk disimpan pada tingkat kolam kapasitas, kami sarankan untuk menggunakan rasio konservatif 1 GiB penyimpanan SSD untuk setiap 10 GiB data yang Anda rencanakan untuk disimpan pada tingkat kolam kapasitas.

Data file yang disimpan di tingkat SSD Anda

Selain kumpulan data aktif Anda dan semua metadata file, semua data yang ditulis ke sistem file Anda pada awalnya ditulis ke tingkat SSD sebelum di-tiered-off ke penyimpanan kolam kapasitas. Hal ini berlaku terlepas dari kebijakan tingkatan volume, dengan pengecualian mentransfer data menggunakan SnapMirror ke volume yang dikonfigurasi dengan kebijakan tiering Semua data.

Pembacaan acak dari tingkat kolam kapasitas di-cache di tingkat SSD, selama tingkat SSD di bawah pemanfaatan 90%. Untuk informasi selengkapnya, lihat Tingkat data volume.

Pemanfaatan kapasitas SSD yang disarankan

Kami menyarankan agar Anda tidak melebihi 80% pemanfaatan tingkat penyimpanan SSD Anda secara berkelanjutan. Untuk sistem file scale-out, kami juga menyarankan agar Anda tidak melebihi 80% pemanfaatan agregat sistem file Anda secara berkelanjutan. Rekomendasi ini konsisten dengan NetApp rekomendasi untuk ONTAP. Karena tingkat SSD sistem file Anda juga digunakan untuk pementasan penulisan, dan untuk pembacaan acak dari, tingkat kumpulan kapasitas, setiap perubahan mendadak dalam pola akses dapat dengan cepat menyebabkan pemanfaatan tingkat SSD Anda meningkat.

Pada pemanfaatan SSD 90%, data yang dibaca dari tier pool kapasitas tidak lagi di-cache pada tingkat SSD sehingga kapasitas SSD yang tersisa dipertahankan untuk setiap data baru yang ditulis ke sistem file. Hal ini menyebabkan pembacaan berulang data yang sama dari tingkat kumpulan kapasitas dibaca dari penyimpanan kumpulan kapasitas alih-alih di-cache dan dibaca dari tingkat SSD, yang dapat memengaruhi kapasitas throughput sistem file Anda.

Semua fungsionalitas tiering berhenti ketika tingkat SSD berada pada atau di atas pemanfaatan 98%. Untuk informasi selengkapnya, lihat Ambang batas jenjang.

fsX untuk efisiensi penyimpanan ONTAP

NetApp ONTAP menawarkan fitur efisiensi penyimpanan tingkat blok termasuk kompresi, pemadatan, dan deduplikasi yang dapat menghemat hingga 65% dalam kapasitas penyimpanan untuk berbagi file umum, tanpa mengorbankan kinerja.

Amazon FSx untuk NetApp ONTAP juga mendukung fitur ONTAP lain yang menghemat ruang Anda, termasuk snapshot, penyediaan tipis, dan volume. FlexClone

Fitur efisiensi penyimpanan tidak diaktifkan secara default. Anda dapat mengaktifkannya sebagai berikut:

- Pada volume root SVM saat Anda membuat sistem file.
- Saat Anda membuat volume baru.
- Saat Anda memodifikasi volume yang ada.

Untuk melihat jumlah penghematan penyimpanan pada sistem file dengan efisiensi penyimpanan diaktifkan, lihatMelihat penghematan efisiensi penyimpanan.

Menghitung penghematan efisiensi penyimpanan

Anda dapat menggunakan `LogicalDataStored` dan `StorageUsed` fsX untuk metrik sistem CloudWatch file ONTAP untuk menghitung penghematan penyimpanan dari kompresi, deduplikasi, pemadatan, snapshot, dan. FlexClones Metrik ini memiliki dimensi tunggal,`FileSystemId`. Untuk informasi selengkapnya, lihat Metrik sistem file.

- Untuk menghitung penghematan efisiensi penyimpanan dalam byte, ambil Rata-rata `StorageUsed` selama periode tertentu dan kurangi dari Rata-rata selama periode yang sama. `LogicalDataStored`
- Untuk menghitung penghematan efisiensi penyimpanan sebagai persentase dari total ukuran data logis, ambil `Average` dari `StorageUsed` selama periode tertentu dan kurangi dari `LogicalDataStored` periode yang sama`Average`. Kemudian bagi perbedaannya `Average` dengan `LogicalDataStored` periode yang sama.

Contoh ukuran SSD

Asumsikan Anda ingin menyimpan 100 TiB data untuk aplikasi di mana 80% data jarang diakses. Dalam skenario ini, 80% (80 TB) data Anda secara otomatis berjenjang ke tingkat kolam kapasitas dan 20% sisanya (20 TB) tetap dalam penyimpanan SSD. Berdasarkan penghematan efisiensi penyimpanan tipikal sebesar 65% untuk beban kerja berbagi file tujuan umum, yang setara dengan 7 TiB data. Untuk mempertahankan tingkat pemanfaatan SSD 80%, Anda memerlukan kapasitas penyimpanan SSD 8,75 TiB untuk 20 TiB data yang diakses secara aktif. Jumlah penyimpanan SSD yang Anda berikan juga perlu memperhitungkan overhead penyimpanan perangkat lunak ONTAP sebesar 16%, seperti yang ditunjukkan dalam perhitungan berikut.

```
ssdNeeded = ssdProvisioned * (1 - 0.16)
8.75 TiB / 0.84 = ssdProvisioned
10.42 TiB = ssdProvisioned
```

Jadi dalam contoh ini, Anda perlu menyediakan setidaknya 10,42 TiB penyimpanan SSD. Anda juga akan menggunakan 28 TiB penyimpanan kolam kapasitas untuk sisa 80 TiB data yang jarang diakses.

Kapasitas penyimpanan sistem file dan IOPS

Saat Anda membuat FSx untuk sistem file ONTAP, Anda menentukan kapasitas penyimpanan tingkat SSD. Untuk sistem file scale-out, kapasitas penyimpanan yang Anda tentukan tersebar merata di antara kumpulan penyimpanan dari setiap pasangan ketersediaan tinggi (HA); kumpulan penyimpanan ini disebut agregat.

Untuk setiap GiB penyimpanan SSD yang Anda sediakan, Amazon FSx secara otomatis menyediakan 3 operasi input/output SSD per detik (IOPS) untuk sistem file, hingga maksimum 160.000 IOPS SSD per sistem file. Untuk sistem file scale-out, IOPS SSD Anda tersebar merata di setiap agregat sistem file Anda. Anda memiliki opsi untuk menentukan tingkat IOPS SSD yang disediakan di atas IOPS 3 SSD otomatis per GiB. Untuk informasi selengkapnya tentang jumlah maksimum IOPS SSD yang dapat Anda berikan untuk FSx untuk sistem file ONTAP, lihat. Dampak kapasitas throughput terhadap performa

Topik

- Memperbarui penyimpanan SSD sistem file dan IOPS
- Memantau pemanfaatan penyimpanan SSD

- Membuat sistem file Alarm Pemanfaatan Kapasitas Penyimpanan
- Melihat penghematan efisiensi penyimpanan
- Memodifikasi kapasitas penyimpanan SSD dan IOPS yang disediakan
- Memantau kapasitas penyimpanan dan pembaruan IOPS
- Meningkatkan kapasitas penyimpanan SSD secara dinamis

Memperbarui penyimpanan SSD sistem file dan IOPS

Saat Anda membutuhkan penyimpanan tambahan untuk bagian aktif kumpulan data Anda, Anda dapat meningkatkan kapasitas penyimpanan SSD Amazon FSx Anda untuk sistem file NetApp ONTAP. Gunakan konsol Amazon FSx, Amazon FSx API, atau AWS Command Line Interface (AWS CLI) untuk meningkatkan kapasitas penyimpanan SSD. Untuk informasi selengkapnya, lihat Memodifikasi kapasitas penyimpanan SSD dan IOPS yang disediakan.

Saat Anda meningkatkan kapasitas penyimpanan SSD dari sistem file Amazon FSx Anda, kapasitas baru biasanya tersedia untuk digunakan dalam beberapa menit. Anda ditagih untuk kapasitas penyimpanan SSD baru setelah tersedia untuk Anda. Untuk informasi selengkapnya tentang harga, lihat Amazon FSx untuk Harga NetApp ONTAP.

Setelah Anda meningkatkan kapasitas penyimpanan, Amazon FSx menjalankan proses pengoptimalan penyimpanan di latar belakang untuk menyeimbangkan kembali data Anda. Untuk sebagian besar sistem file, pengoptimalan penyimpanan membutuhkan waktu beberapa jam, dengan dampak nyata minimal terhadap kinerja beban kerja Anda.

Anda dapat melacak kemajuan proses pengoptimalan penyimpanan kapan saja dengan menggunakan konsol Amazon FSx, CLI, dan API. Untuk informasi selengkapnya, lihat Memantau kapasitas penyimpanan dan pembaruan IOPS.

Pertimbangan

Berikut adalah beberapa hal penting yang perlu dipertimbangkan saat memodifikasi kapasitas penyimpanan SSD sistem file dan IOPS yang disediakan:

- Kapasitas penyimpanan hanya meningkat — Anda hanya dapat meningkatkan jumlah kapasitas penyimpanan SSD untuk sistem file; Anda tidak dapat mengurangi kapasitas penyimpanan.
- Peningkatan kapasitas penyimpanan minimum - Setiap peningkatan kapasitas penyimpanan SSD harus minimal 10 persen dari kapasitas penyimpanan SSD sistem file saat ini, hingga kapasitas penyimpanan SSD maksimum untuk konfigurasi sistem file Anda.

- (Scale-out only) Penyebaran kapasitas penyimpanan — Kapasitas penyimpanan baru atau IOPS SSD yang Anda pilih untuk sistem file Anda tersebar merata di setiap agregat sistem file Anda.
- Waktu antara peningkatan — Setelah memodifikasi kapasitas penyimpanan SSD, IOPS yang disediakan, atau kapasitas throughput pada sistem file, Anda harus menunggu setidaknya enam jam sebelum memodifikasi konfigurasi ini pada sistem file yang sama lagi. Ini terkadang disebut sebagai periode pendinginan.
- Mode IOPS yang disediakan — Untuk perubahan IOPS yang disediakan, Anda harus menentukan salah satu dari dua mode IOPS:
  - Mode otomatis - Amazon FSx secara otomatis menskalakan IOPS SSD Anda untuk mempertahankan 3 IOPS SSD yang disediakan per GiB kapasitas penyimpanan SSD, hingga IOPS SSD maksimum untuk konfigurasi sistem file Anda.

    > **Note**
    >
    > Untuk informasi selengkapnya tentang jumlah maksimum IOPS SSD yang dapat Anda berikan untuk FSx untuk sistem file ONTAP, lihat. Dampak kapasitas throughput terhadap performa

  - Mode yang disediakan pengguna - Anda menentukan jumlah IOPS SSD, yang harus lebih besar dari atau sama dengan 3 IOPS per GiB kapasitas penyimpanan SSD. Jika Anda memilih untuk memberikan tingkat IOPS yang lebih tinggi, Anda membayar IOPS rata-rata yang disediakan di atas tarif yang disertakan untuk bulan tersebut, diukur dalam IOP-bulan.

Untuk informasi selengkapnya tentang harga, lihat Amazon FSx untuk Harga NetApp ONTAP.

Kapan meningkatkan kapasitas penyimpanan SSD

Jika Anda kehabisan penyimpanan tingkat SSD yang tersedia, kami sarankan Anda meningkatkan kapasitas penyimpanan sistem file Anda. Kehabisan penyimpanan menunjukkan bahwa tingkat SSD Anda berukuran terlalu kecil untuk bagian aktif kumpulan data Anda.

Untuk memantau jumlah penyimpanan gratis yang tersedia di sistem file, gunakan metrik tingkat sistem file dan `StorageCapacity` `StorageUsed` Amazon CloudWatch . Anda dapat membuat CloudWatch alarm pada metrik dan diberi tahu saat turun di bawah ambang batas tertentu. Untuk informasi selengkapnya, lihat Pemantauan CloudWatch dengan Amazon.

> **Note**
>
> Kami menyarankan agar Anda tidak melebihi 80% pemanfaatan kapasitas penyimpanan SSD untuk memastikan bahwa tiering data, penskalaan throughput, dan aktivitas pemeliharaan lainnya berfungsi dengan baik, dan bahwa ada kapasitas yang tersedia untuk data tambahan. Untuk sistem file scale-out, rekomendasi ini berlaku untuk pemanfaatan rata-rata di semua agregat sistem file Anda dan untuk setiap agregat individu.

Untuk informasi selengkapnya tentang bagaimana penyimpanan SSD sistem file digunakan dan berapa banyak penyimpanan SSD yang dicadangkan untuk metadata file dan perangkat lunak operasi, lihat. Memilih jumlah penyimpanan SSD sistem file yang tepat

Memantau pemanfaatan penyimpanan SSD

Anda dapat memantau pemanfaatan kapasitas penyimpanan SSD sistem file Anda menggunakan berbagai AWS NetApp alat. Menggunakan Amazon, CloudWatch Anda dapat memantau pemanfaatan kapasitas penyimpanan dan menyetel alarm untuk mengingatkan Anda ketika pemanfaatan kapasitas penyimpanan mencapai ambang batas yang dapat disesuaikan.

> **Note**
>
> Kami menyarankan agar Anda tidak melebihi 80% pemanfaatan kapasitas penyimpanan dari tingkat penyimpanan SSD Anda. Ini memastikan bahwa tiering berfungsi dengan benar, dan menyediakan overhead untuk data baru. Jika tingkat penyimpanan SSD Anda secara konsisten di atas pemanfaatan kapasitas penyimpanan 80%, Anda dapat meningkatkan kapasitas tingkat penyimpanan SSD Anda. Untuk informasi selengkapnya, lihat Memperbarui penyimpanan SSD sistem file dan IOPS.

Anda dapat melihat penyimpanan SSD sistem file yang tersedia dan distribusi penyimpanan keseluruhan di konsol Amazon FSx. Grafik kapasitas penyimpanan SSD yang Tersedia menampilkan jumlah kapasitas penyimpanan berbasis SSD yang tersedia pada sistem file dari waktu ke waktu. Grafik distribusi Storage menunjukkan bagaimana kapasitas penyimpanan keseluruhan sistem file saat ini didistribusikan lebih dari 3 kategori:

- Tingkat kolam kapasitas
- SSD tier - tersedia

- SSD tier - digunakan

Anda dapat memantau pemanfaatan kapasitas penyimpanan SSD sistem file Anda di AWS Management Console, menggunakan prosedur berikut.

Untuk memantau sistem file tersedia kapasitas penyimpanan SSD tier (konsol)

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Pilih Sistem file di kolom navigasi sebelah kiri, lalu pilih sistem ONTAP file yang ingin Anda lihat informasi kapasitas penyimpanan. Halaman detail sistem file muncul.
3. Di panel kedua, pilih tab Monitoring & performance, lalu pilih Storage. Kapasitas penyimpanan utama yang tersedia dan pemanfaatan kapasitas Penyimpanan per grafik agregat ditampilkan.

Membuat sistem file Alarm Pemanfaatan Kapasitas Penyimpanan

Kami menyarankan agar Anda tidak melebihi pemanfaatan kapasitas penyimpanan SSD rata-rata 80% secara berkelanjutan. Lonjakan pemanfaatan penyimpanan SSD sesekali di atas 80% dapat diterima. Mempertahankan penggunaan rata-rata di bawah 80% memberi Anda kapasitas yang cukup untuk meningkatkan penyimpanan Anda tanpa mengalami masalah. Prosedur berikut menunjukkan cara membuat CloudWatch alarm yang memberi tahu Anda kapan penggunaan penyimpanan SSD sistem file Anda mendekati 80%.

Untuk membuat alarm SCU sistem file

Anda dapat menggunakan `StorageCapacityUtilization` metrik untuk membuat alarm yang dipicu ketika satu atau lebih dari FSx Anda untuk sistem file ONTAP telah mencapai ambang batas pemanfaatan penyimpanan.

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi kiri, di bawah Alarm, pilih Semua alarm. Kemudian, pilih Buat alarm. Dalam wizard buat alarm, pilih Pilih metrik.
3. Di penjelajah grafik, pilih tab Kueri multi sumber.
4. Di pembuat kueri, pilih yang berikut ini:
   - Untuk Namespace, pilih AWS/FSx > Metrik Sistem File Terperinci.
   - Untuk nama Metrik, pilih MAX (StorageCapacityUtilization).

- Untuk Filter by, Anda dapat secara opsional menyertakan atau mengecualikan sistem file tertentu dengan ID mereka. Jika Anda membiarkan Filter kosong, alarm Anda akan terpicu ketika salah satu sistem file Anda melebihi ambang batas pemanfaatan kapasitas penyimpanan alarm Anda.
- Biarkan sisa opsi kosong, dan pilih Kueri grafik.

5. Pilih Pilih Metrik. Kembali ke wizard, di bagian Metrik, berikan label pada metrik Anda. Kami merekomendasikan untuk menjaga Periode hingga 5 menit.
6. Di bawah Kondisi, pilih jenis ambang Statis, setiap kali metrik Anda lebih besar/sama dengan 80.
7. Pilih Berikutnya untuk pergi ke halaman Configure actions.

Untuk mengkonfigurasi tindakan alarm

Anda dapat mengonfigurasi berbagai tindakan agar alarm dapat dipicu saat mencapai ambang batas yang Anda konfigurasikan. Dalam contoh ini, kami memilih topik Simple Notification Service (SNS), tetapi Anda dapat mempelajari tentang tindakan lain di Menggunakan CloudWatch alarm Amazon di Panduan Pengguna Amazon. CloudWatch

1. Di bagian Pemberitahuan, pilih topik SNS untuk memberi tahu saat alarm Anda dalam status. `ALARM` Anda dapat memilih topik yang ada atau membuat yang baru. Anda akan menerima pemberitahuan berlangganan yang perlu Anda konfirmasi sebelum menerima pemberitahuan alarm ke alamat email.
2. Pilih Selanjutnya.

Untuk menyelesaikan alarm

Ikuti petunjuk ini untuk menyelesaikan proses pembuatan CloudWatch alarm Anda.

1. Pada halaman Tambahkan nama dan deskripsi, beri nama alarm Anda, dan deskripsi opsional, lalu pilih Berikutnya.
2. Tinjau semua yang telah Anda konfigurasi di halaman Pratinjau dan buat, lalu pilih Buat alarm.

Melihat penghematan efisiensi penyimpanan

Saat diaktifkan, Anda dapat melihat berapa banyak kapasitas penyimpanan yang Anda hemat di konsol Amazon FSx, CloudWatch konsol Amazon, dan CLI ONTAP.

Untuk melihat penghematan efisiensi penyimpanan (konsol)

Penghematan efisiensi penyimpanan yang ditampilkan di konsol Amazon FSx untuk sistem file FSx untuk ONTAP mencakup penghematan dari dan. FlexClones SnapShots

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Pilih sistem file FSx untuk ONTAP yang ingin Anda lihat penghematan efisiensi penyimpanan dari daftar sistem File.
3. Pilih Ringkasan di tab Pemantauan & kinerja pada panel kedua di halaman detail sistem file.
4. Bagan penghematan efisiensi penyimpanan menunjukkan berapa banyak ruang yang Anda hemat sebagai persentase dari ukuran data logis Anda dan dalam byte fisik.

Untuk melihat penghematan efisiensi penyimpanan (ONTAPCLI)

Anda dapat melihat penghematan efisiensi penyimpanan hanya dari pemadatan, kompresi, dan deduplikasi — tanpa efek snapshot dan FlexClones — dengan menjalankan perintah `storage aggregate show-efficiency` menggunakan CLI. ONTAP Untuk informasi selengkapnya, lihat efisiensi pertunjukan agregat penyimpanan di Pusat Dokumentasi. NetApp ONTAP

1. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen Amazon fsX NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *`management_endpoint_ip`* dengan alamat IP port manajemen sistem file.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Untuk informasi selengkapnya, lihat Mengelola sistem file dengan ONTAP CLI.
2. storage aggregate show-efficiencyPerintah menampilkan informasi tentang efisiensi penyimpanan semua agregat. Efisiensi penyimpanan ditampilkan pada empat tingkatan yang berbeda:

   - Total
   - Agregat
   - Volume
   - Snapshot dan volume FlexClone

```
::*> aggr show-efficiency

Aggregate: aggr1
     Node: node1

Total Data Reduction Efficiency Ratio:  3.29:1
Total Storage Efficiency Ratio:         4.29:1
Aggregate: aggr2
     Node: node1

Total Data Reduction Efficiency Ratio:  4.50:1
Total Storage Efficiency Ratio:         5.49:1

cluster::*> aggr show-efficiency -details

Aggregate: aggr1
     Node: node1

Total Data Reduction Ratio:                    2.39:1
Total Storage Efficiency Ratio:                4.29:1

Aggregate level Storage Efficiency
(Aggregate Deduplication and Data Compaction): 1.00:1
Volume Deduplication Efficiency:               5.03:1
Compression Efficiency:                        1.00:1

Snapshot Volume Storage Efficiency:            8.81:1
FlexClone Volume Storage Efficiency:           1.00:1
Number of Efficiency Disabled Volumes:         1

Aggregate: aggr2
     Node: node1
Total Data Reduction Ratio:                    2.39:1
Total Storage Efficiency Ratio:                4.29:1

Aggregate level Storage Efficiency
(Aggregate Deduplication and Data Compaction): 1.00:1
Volume Deduplication Efficiency:               5.03:1
Compression Efficiency:                        1.00:1

Snapshot Volume Storage Efficiency:            8.81:1
FlexClone Volume Storage Efficiency:           1.00:1
```

```
Number of Efficiency Disabled Volumes:         1
```

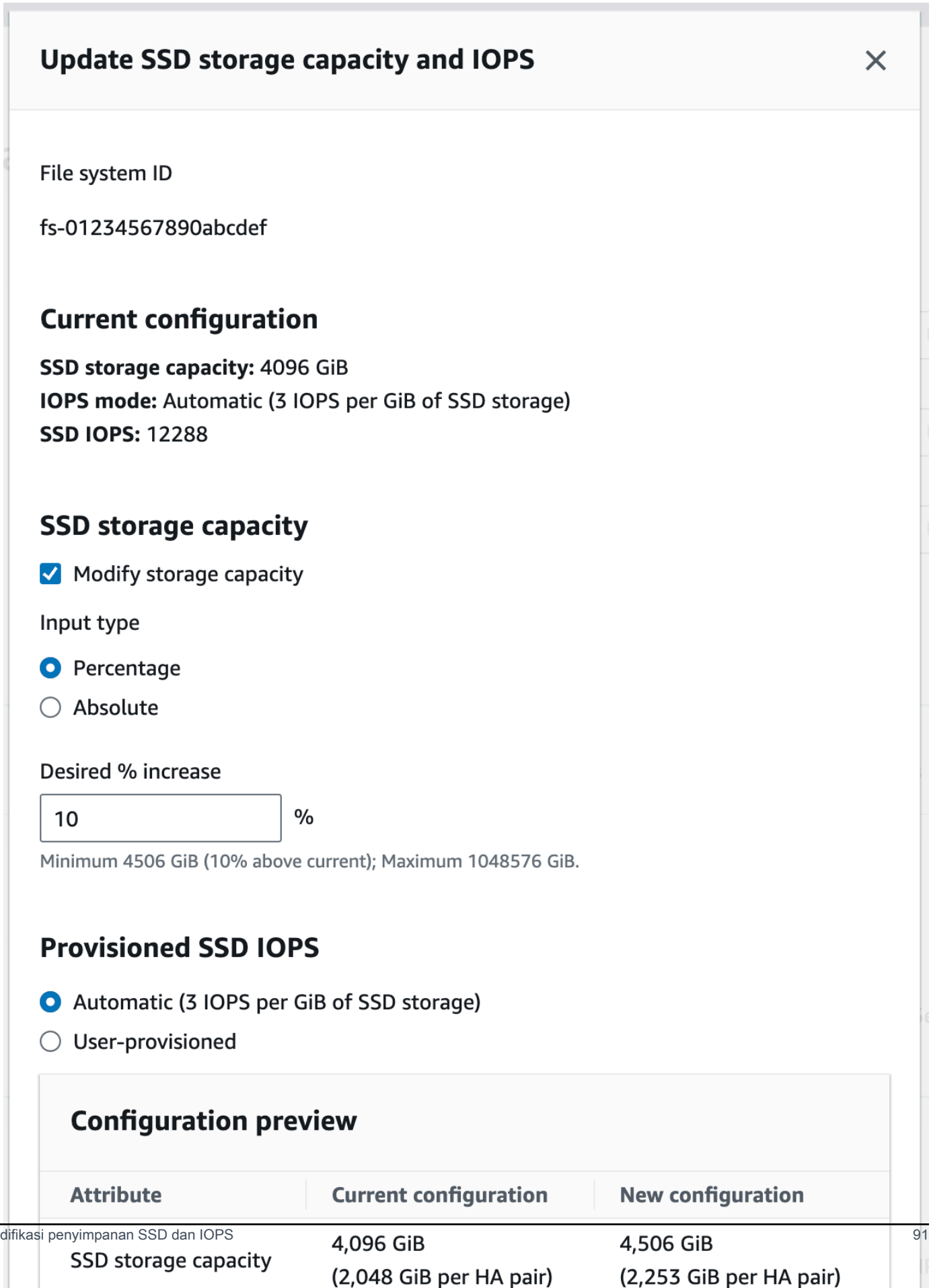
Memodifikasi kapasitas penyimpanan SSD dan IOPS yang disediakan

Anda dapat meningkatkan penyimpanan berbasis SSD sistem file, dan Anda menambah atau mengurangi jumlah IOPS SSD yang disediakan dengan menggunakan konsol Amazon FSx, API, dan. AWS CLI

Untuk memperbarui kapasitas penyimpanan SSD atau IOPS yang disediakan untuk sistem file (konsol)

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Di panel navigasi kiri, pilih Sistem file. Dalam daftar Sistem file, pilih FSx untuk sistem file ONTAP yang ingin Anda perbarui kapasitas penyimpanan SSD dan SSD IOPS.
3. Pilih Tindakan > Perbarui kapasitas penyimpanan. Atau, di bagian Ringkasan, pilih Perbarui di sebelah nilai kapasitas penyimpanan SSD sistem file.

   Perbarui kapasitas penyimpanan SSD dan kotak dialog IOPS muncul.


Update SSD storage capacity and IOPS
File system ID
fs-01234567890abcdef
Current configuration
SSD storage capacity: 4096 GiB
IOPS mode: Automatic (3 IOPS per GiB of SSD storage)
SSD IOPS: 12288
SSD storage capacity
Modify storage capacity
Input type
Percentage
Absolute
Desired % increase
10
%
Minimum 4506 GiB (10% above current); Maximum 1048576 GiB.
Provisioned SSD IOPS
Automatic (3 IOPS per GiB of SSD storage)
User-provisioned
Configuration preview
Attribute
Current configuration
New configuration
SSD storage capacity
4,096 GiB
(2,048 GiB per HA pair)
4,506 GiB
(2,253 GiB per HA pair)
Mode: Automatic
Mode: Automatic

4. Untuk meningkatkan kapasitas penyimpanan SSD, pilih Ubah kapasitas penyimpanan.
5. Untuk jenis Input, pilih salah satu dari berikut ini:
   - Untuk memasukkan kapasitas penyimpanan SSD baru sebagai persentase perubahan dari nilai saat ini, pilih Persentase.
   - Untuk memasukkan nilai baru di GiB, pilih Absolute.
6. Tergantung pada jenis input, masukkan nilai untuk kenaikan% yang diinginkan.
   - Untuk Persentase, masukkan nilai kenaikan persentase. Nilai ini harus setidaknya 10 persen lebih besar dari nilai saat ini.
   - Untuk Absolute, masukkan nilai baru di GiB, hingga nilai maksimum yang diizinkan 196.608 GiB.
7. Untuk Provisioned SSD IOPS, Anda memiliki dua opsi untuk mengubah jumlah IOPS SSD yang disediakan untuk sistem file Anda:
   - Jika Anda ingin Amazon FSx secara otomatis menskalakan IOPS SSD Anda untuk mempertahankan 3 IOPS SSD yang disediakan per GiB kapasitas penyimpanan SSD (hingga maksimum 160.000), pilih Otomatis.
   - Jika Anda ingin menentukan jumlah IOPS SSD, pilih User-provisioned. Masukkan jumlah absolut IOPS yang setidaknya tiga kali jumlah GiB dari tingkat penyimpanan SSD Anda, dan kurang dari atau sama dengan 160.000.

> **Note**
>
> Untuk informasi selengkapnya tentang jumlah maksimum IOPS SSD yang dapat Anda berikan untuk FSx untuk sistem file ONTAP, lihat. Dampak kapasitas throughput terhadap performa

8. Pilih Perbarui.

> **Note**
>
> Di bagian bawah prompt, pratinjau konfigurasi ditampilkan untuk kapasitas penyimpanan SSD baru Anda dan IOPS SSD. Untuk sistem file scale-out, nilai per-HA-pair juga ditampilkan.

Untuk memperbarui kapasitas penyimpanan SSD dan IOPS yang disediakan untuk sistem file (CLI)

Untuk memperbarui kapasitas penyimpanan SSD dan IOPS yang disediakan untuk sistem file FSx untuk ONTAP, gunakan AWS CLI perintah update-file-systematau tindakan API yang setara. UpdateFileSystem Tetapkan parameter berikut dengan nilai Anda:

- Atur `--file-system-id` ke ID dari sistem file yang Anda perbarui.
- Untuk meningkatkan kapasitas penyimpanan SSD Anda, atur `--storage-capacity` ke nilai kapasitas penyimpanan target, yang harus setidaknya 10 persen lebih besar dari nilai saat ini.
- Untuk memodifikasi IOPS SSD yang disediakan, gunakan properti. `--ontap-configuration` `DiskIopsConfiguration` Properti ini memiliki dua parameter, `Iops` dan`Mode`:
  - Jika Anda ingin menentukan jumlah IOPS yang disediakan, gunakan `Iops=`*`number_of_IOPS`* (hingga maksimum 160.000) dan. `Mode=USER_PROVISIONED` Nilai IOPS harus lebih besar dari atau sama dengan tiga kali kapasitas penyimpanan SSD yang diminta. Jika Anda tidak meningkatkan kapasitas penyimpanan, nilai IOP harus lebih besar dari atau sama dengan tiga kali kapasitas penyimpanan SSD saat ini.
  - Jika Anda ingin Amazon FSx meningkatkan IOPS SSD Anda secara otomatis, gunakan `Mode=AUTOMATIC` dan jangan gunakan parameternya. `Iops` Amazon FSx akan secara otomatis mempertahankan 3 IOPS SSD per GiB dari kapasitas penyimpanan SSD yang disediakan (hingga maksimum 160.000).

> **Note**
>
> Untuk informasi selengkapnya tentang jumlah maksimum IOPS SSD yang dapat Anda berikan untuk FSx untuk sistem file ONTAP, lihat. Dampak kapasitas throughput terhadap performa

Contoh berikut meningkatkan penyimpanan SSD sistem file menjadi 2000 GiB dan menetapkan jumlah IOPS SSD yang disediakan pengguna menjadi 7000.

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--storage-capacity 2000 \
--ontap-configuration 'DiskIopsConfiguration={Iops=7000,Mode=USER_PROVISIONED}'
```

Untuk memantau kemajuan pembaruan, gunakan describe-file-systems AWS CLI perintah. Cari `AdministrativeActions` bagian dalam output.

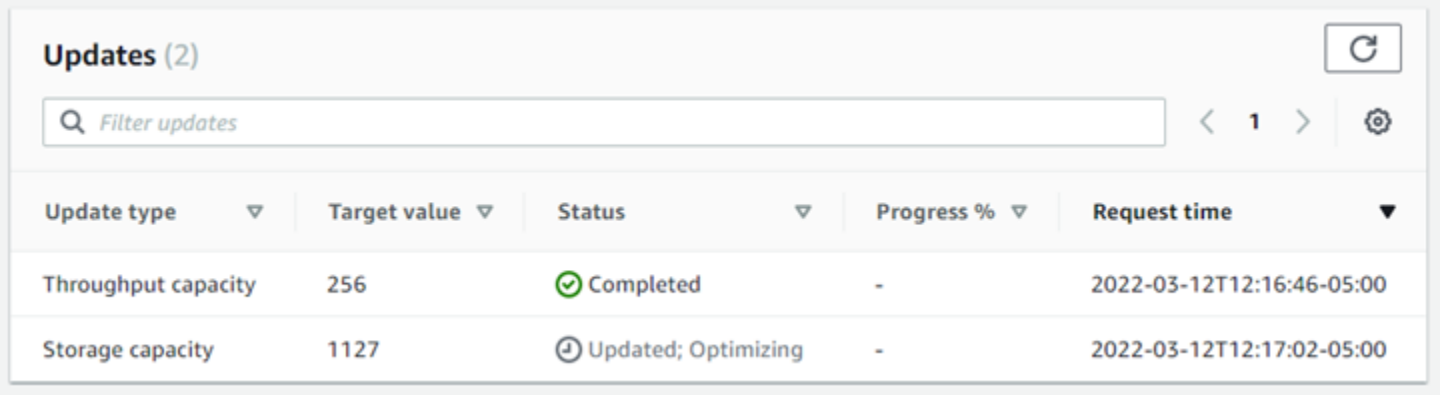
Untuk informasi selengkapnya, lihat AdministrativeActiondi Amazon FSx untuk Referensi API NetApp ONTAP.

Memantau kapasitas penyimpanan dan pembaruan IOPS

Anda dapat memantau kemajuan kapasitas penyimpanan SSD dan pembaruan IOPS dengan menggunakan konsol Amazon FSx, CLI, dan API.

Untuk memantau penyimpanan dan pembaruan IOPS (konsol)

Di tab Pembaruan pada halaman detail sistem file untuk FSx Anda untuk sistem file ONTAP, Anda dapat melihat 10 pembaruan terbaru untuk setiap jenis pembaruan.



Untuk kapasitas penyimpanan SSD dan pembaruan IOPS, Anda dapat melihat informasi berikut:

Jenis pembaruan

Jenis yang didukung adalah Kapasitas penyimpanan, Mode, dan IOPS. Nilai Mode dan IOPS terdaftar untuk semua kapasitas penyimpanan dan permintaan penskalaan IOPS.

Nilai target

Nilai yang Anda tentukan untuk memperbarui kapasitas penyimpanan SSD sistem file atau IOPS ke.

Status

Status terkini dari pembaruan. Kemungkinan nilainya adalah sebagai berikut:

- Tertunda - Amazon FSx menerima permintaan pembaruan, tetapi belum mulai memprosesnya.
- Dalam proses – Amazon FSx sedang memproses permintaan pembaruan.

- Diperbarui; Mengoptimalkan - Amazon FSx meningkatkan kapasitas penyimpanan SSD sistem file. Proses optimasi penyimpanan sekarang menyeimbangkan kembali data Anda di latar belakang.
- Selesai - Pembaruan selesai dengan sukses.
- Gagal — Permintaan pembaruan gagal. Pilih tanda tanya (?) untuk melihat detailnya.

Kemajuan%

Menampilkan kemajuan proses pengoptimalan penyimpanan saat persentase selesai.

Waktu permintaan

Waktu Amazon FSx menerima permintaan tindakan pembaruan.

Untuk memantau penyimpanan dan pembaruan IOPS (CLI)

Anda dapat melihat dan memantau permintaan peningkatan kapasitas penyimpanan SSD sistem file dengan menggunakan describe-file-systems AWS CLI perintah dan operasi DescribeFileSystemsAPI. Array `AdministrativeActions` mencantumkan 10 tindakan pembaruan terbaru untuk setiap jenis tindakan administratif. Saat Anda meningkatkan kapasitas penyimpanan SSD sistem file, dua `AdministrativeActions` tindakan dihasilkan: a `FILE_SYSTEM_UPDATE` dan `STORAGE_OPTIMIZATION` tindakan.

Contoh berikut menunjukkan kutipan respons perintah CLI `describe-file-systems`. Sistem file memiliki tindakan administratif yang tertunda untuk meningkatkan kapasitas penyimpanan SSD menjadi 2000 GiB dan IOPS SSD yang disediakan menjadi 7000.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586797629.095,
        "Status": "PENDING",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
             }
        }
```

```
    },
    {
        "AdministrativeActionType": "STORAGE_OPTIMIZATION",
        "RequestTime": 1586797629.095,
        "Status": "PENDING"
    }
]
```

Amazon FSx memproses tindakan `FILE_SYSTEM_UPDATE` terlebih dahulu, menambahkan disk penyimpanan baru yang lebih besar ke sistem file. Ketika penyimpanan baru tersedia untuk sistem file, status `FILE_SYSTEM_UPDATE` berubah menjadi `UPDATED_OPTIMIZING`. Kapasitas penyimpanan menunjukkan nilai baru yang lebih besar, dan Amazon FSx mulai memproses tindakan administratif `STORAGE_OPTIMIZATION`. Perilaku ini ditunjukkan dalam kutipan berikut dari respons perintah CLI`describe-file-systems`.

`ProgressPercent`Properti menampilkan kemajuan proses optimasi penyimpanan. Setelah proses pengoptimalan penyimpanan berhasil diselesaikan, status `FILE_SYSTEM_UPDATE` tindakan berubah menjadi`COMPLETED`, dan `STORAGE_OPTIMIZATION` tindakan tidak lagi muncul.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586799169.445,
        "Status": "UPDATED_OPTIMIZING",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
            }
        }
    },
    {
        "AdministrativeActionType": "STORAGE_OPTIMIZATION",
        "ProgressPercent": 41,
        "RequestTime": 1586799169.445,
        "Status": "IN_PROGRESS"
    }
]
```

Jika kapasitas penyimpanan atau permintaan pembaruan IOPS gagal, status `FILE_SYSTEM_UPDATE` tindakan berubah menjadi`FAILED`, seperti yang ditunjukkan pada contoh berikut. `FailureDetails`Properti memberikan informasi tentang kegagalan.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586373915.697,
        "Status": "FAILED",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
            }
        },
        "FailureDetails": {
            "Message": "failure-message"
        }
    }
]
```

Meningkatkan kapasitas penyimpanan SSD secara dinamis

Anda dapat menggunakan solusi berikut untuk secara dinamis meningkatkan kapasitas penyimpanan SSD dari FSx untuk sistem file ONTAP ketika jumlah kapasitas penyimpanan SSD yang digunakan melebihi ambang batas yang Anda tentukan. AWS CloudFormation Template ini secara otomatis menyebarkan semua komponen yang diperlukan untuk menentukan ambang kapasitas penyimpanan, CloudWatch alarm Amazon berdasarkan ambang batas ini, dan AWS Lambda fungsi yang meningkatkan kapasitas penyimpanan sistem file.

Solusinya secara otomatis menyebarkan semua komponen yang dibutuhkan, dan menggunakan parameter berikut:

- FSx Anda untuk ID sistem file ONTAP.
- Ambang kapasitas penyimpanan SSD yang digunakan (nilai numerik). Ini adalah persentase di mana CloudWatch alarm akan dipicu.
- Persentase yang digunakan untuk meningkatkan kapasitas penyimpanan (%).

- Alamat email yang digunakan untuk menerima pemberitahuan penskalaan.

Topik

Gambaran umum arsitektur

Men-deploy solusi ini untuk membangun sumber daya berikut di AWS Cloud.

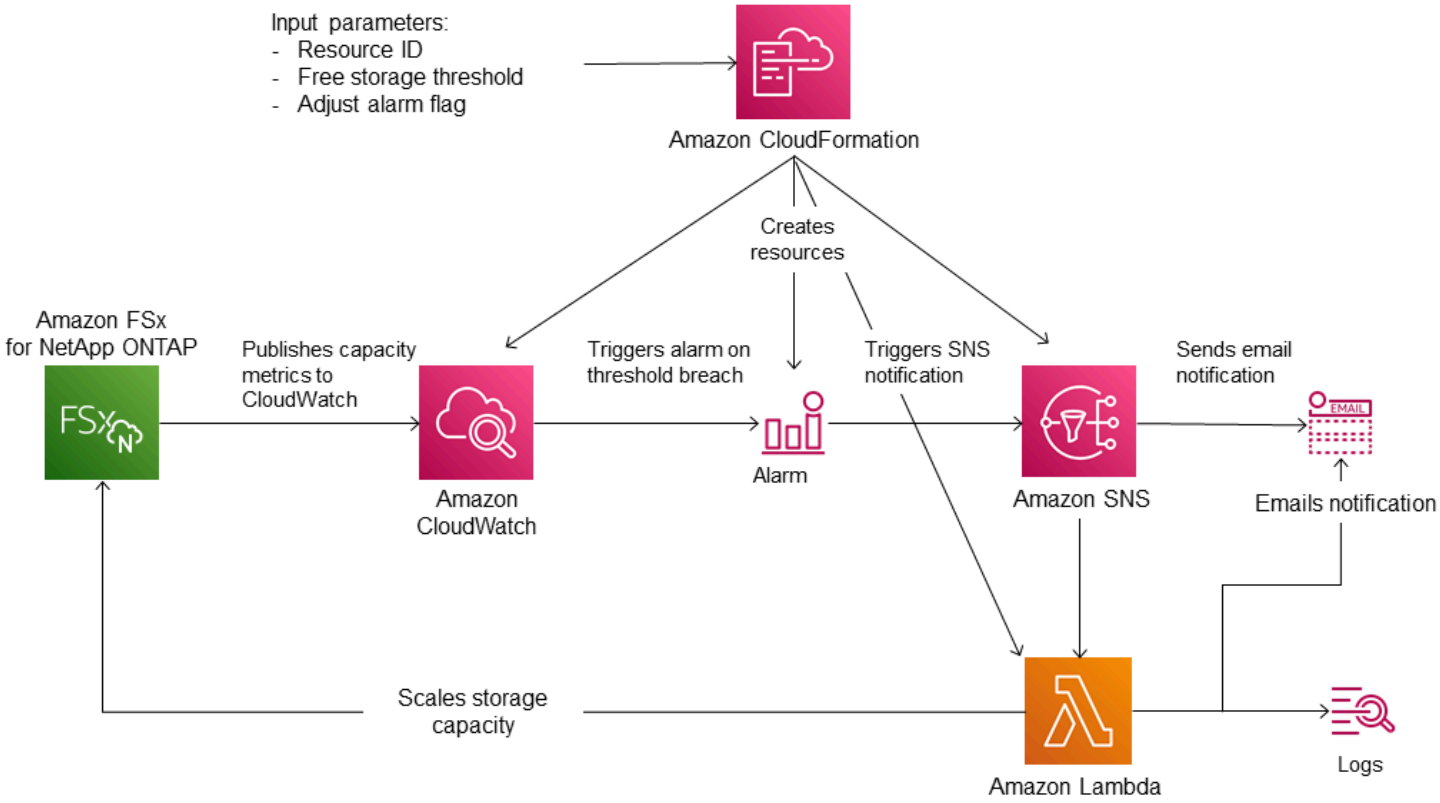


Diagram ini menggambarkan langkah-langkah berikut:

1. AWS CloudFormation Template menyebarkan CloudWatch alarm, AWS Lambda fungsi, antrean Amazon Simple Notification Service (Amazon SNS), dan semua peran yang diperlukan (IAM). AWS Identity and Access Management IAM role memberikan izin fungsi Lambda untuk melakukan operasi API Amazon FSx.
2. CloudWatch memicu alarm ketika kapasitas penyimpanan yang digunakan sistem file melebihi ambang batas yang ditentukan, dan mengirim pesan ke antrian Amazon SNS. Alarm dipicu hanya

ketika kapasitas yang digunakan sistem file melebihi ambang batas terus menerus selama periode 5 menit.

3. Solusi tersebut kemudian memicu fungsi Lambda yang terdaftar ke topik Amazon SNS ini.
4. Fungsi Lambda menghitung kapasitas penyimpanan sistem file yang baru berdasarkan nilai peningkatan persen yang ditentukan dan mengatur kapasitas penyimpanan sistem file yang baru.
5. Status CloudWatch alarm asli dan hasil operasi fungsi Lambda dikirim ke antrian Amazon SNS.

Untuk menerima pemberitahuan tentang tindakan yang dilakukan sebagai respons terhadap CloudWatch alarm, Anda harus mengonfirmasi langganan topik Amazon SNS dengan mengikuti tautan yang disediakan di email Konfirmasi Langganan.

AWS CloudFormation Template

Solusi ini digunakan AWS CloudFormation untuk mengotomatiskan penyebaran komponen yang digunakan untuk secara otomatis meningkatkan kapasitas penyimpanan FSx untuk sistem file ONTAP. Untuk menggunakan solusi ini, unduh SxOntapDynamicStorageScaling AWS CloudFormation templat F.

Template tersebut menggunakan Parameter yang dideskripsikan sebagai berikut. Tinjau parameter templat dan nilai-nilai default-nya, dan modifikasi templat-templat tersebut untuk kebutuhan sistem file Anda.

FileSystemId

Tidak ada nilai default. ID sistem file yang kapasitas penyimpanannya ingin Anda tingkatkan secara otomatis.

LowFreeDataStorageCapacityThreshold

Tidak ada nilai default. Menentukan ambang kapasitas penyimpanan yang digunakan untuk memicu alarm dan secara otomatis meningkatkan kapasitas penyimpanan sistem file, yang ditentukan dalam persentase (%) dari kapasitas penyimpanan sistem file saat ini. Sistem file dianggap memiliki kapasitas penyimpanan gratis yang rendah ketika penyimpanan yang digunakan melebihi ambang batas ini.

EmailAddress

Tidak ada nilai default. Menentukan alamat email yang akan digunakan untuk langganan SNS dan menerima peringatan ambang kapasitas penyimpanan.

PercentIncrease

Defaultnya adalah 20%. Tentukan jumlah yang digunakan untuk meningkatkan kapasitas penyimpanan, yang dinyatakan sebagai persentase dari kapasitas penyimpanan saat ini.

> **Note**
>
> Penskalaan penyimpanan dicoba sekali setiap kali CloudWatch alarm memasuki status. `ALARM` Jika pemanfaatan kapasitas penyimpanan SSD Anda tetap di atas ambang batas setelah operasi penskalaan penyimpanan dicoba, operasi penskalaan penyimpanan tidak dicoba lagi.

MaxF B SxSizeinGi

Defaultnya adalah 196608. Menentukan kapasitas penyimpanan maksimum yang didukung untuk penyimpanan SSD.

Penerapan otomatis dengan AWS CloudFormation

Prosedur berikut mengkonfigurasi dan menyebarkan AWS CloudFormation tumpukan untuk secara otomatis meningkatkan kapasitas penyimpanan FSx untuk sistem file ONTAP. Dibutuhkan beberapa menit untuk menyebarkan. Untuk informasi selengkapnya tentang membuat CloudFormation tumpukan, lihat Membuat tumpukan di AWS CloudFormation konsol di Panduan AWS CloudFormation Pengguna.

> **Note**
>
> Menerapkan solusi ini menimbulkan penagihan untuk layanan terkait. AWS Untuk informasi lebih lanjut, lihat halaman detail harga untuk layanan tersebut.

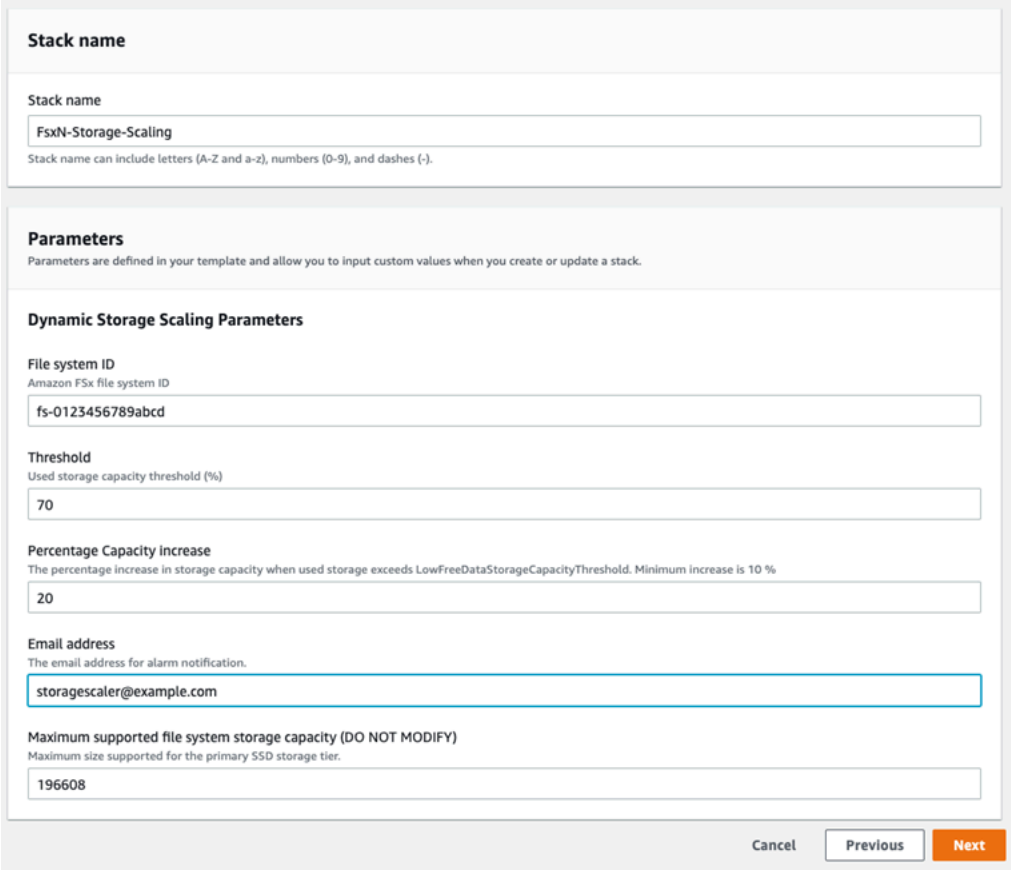
Sebelum memulai, Anda harus memiliki ID sistem file Amazon FSx yang berjalan di Amazon Virtual Private Cloud (Amazon VPC) di situs Anda. Akun AWS Untuk informasi selengkapnya tentang pembuatan sumber daya Amazon FSx, lihat Memulai Amazon FSx untuk ONTAP NetApp .

Untuk meluncurkan kapasitas penyimpanan otomatis yang meningkatkan tumpukan solusi

1. Unduh SxOntapDynamicStorageScaling AWS CloudFormation templat F.

> **Note**
>
> Amazon FSx saat ini hanya tersedia di Wilayah tertentu AWS . Anda harus meluncurkan solusi ini di AWS Wilayah tempat Amazon FSx tersedia. Untuk informasi selengkapnya, lihat titik akhir dan kuota Amazon FSx di. Referensi Umum AWS

2. Dari AWS CloudFormation konsol, pilih Buat tumpukan> Dengan sumber daya baru.
3. Pilih Template sudah siap. Di bagian Tentukan templat, pilih Unggah file templat dan unggah templat yang Anda unduh.
4. Dalam Spesifikasikan detail tumpukan, masukkan nilai untuk solusi peningkatan kapasitas penyimpanan otomatis Anda.



5. Masukkan Nama tumpukan.
6. Untuk Parameter, tinjau parameter untuk templat dan modifikasi untuk memenuhi kebutuhan sistem file Anda. Lalu pilih Selanjutnya.

> **Note**
>
> Untuk menerima pemberitahuan email saat penskalaan dicoba oleh CloudFormation templat ini, konfirmasikan email langganan SNS yang Anda terima setelah menerapkan templat.

7. Masukkan pengaturan Opsi yang Anda inginkan untuk solusi kustom Anda, lalu pilih Berikutnya.
8. Untuk Meninjau, tinjau dan konfirmasikan pengaturan solusi. Pilih kotak centang untuk mengakui bahwa templat membuat sumber daya IAM.
9. Pilih Buat untuk men-deploy tumpukan.

Anda dapat melihat status tumpukan di AWS CloudFormation konsol di kolom Status. Anda akan melihat status CREATE_COMPLETE dalam beberapa menit.

Memperbarui tumpukan

Setelah tumpukan dibuat, Anda dapat memperbaruinya dengan menggunakan templat yang sama dan berikan nilai baru untuk parameternya. Untuk informasi selengkapnya, lihat Memperbarui tumpukan secara langsung di Panduan Pengguna AWS CloudFormation .

Kapasitas penyimpanan volume

FSx untuk volume ONTAP adalah sumber daya virtual yang Anda gunakan untuk mengelompokkan data, menentukan bagaimana data disimpan, dan menentukan jenis akses ke data Anda. Volume, seperti folder, tidak mengkonsumsi kapasitas penyimpanan sistem file itu sendiri. Hanya data yang disimpan dalam volume yang mengkonsumsi penyimpanan SSD dan, tergantung pada kebijakan tingkatan volume, penyimpanan kolam kapasitas. Anda mengatur ukuran volume saat Anda membuatnya, dan Anda dapat mengubah ukurannya nanti. Anda dapat memantau dan mengelola kapasitas penyimpanan FSx Anda untuk volume ONTAP menggunakan AWS Management Console, AWS CLI dan API, dan CLI ONTAP.

Topik

- Mengaktifkan autosizing volume
- Memantau kapasitas penyimpanan volume
- Menyetel kebijakan tingkatan volume
- Mengatur hari pendinginan minimum
- Menyetel kebijakan pengambilan cloud volume
- Melihat kapasitas file volume
- Meningkatkan jumlah maksimum file pada volume
- Mengaktifkan mode tulis cloud volume

Tingkat data volume

Amazon FSx untuk sistem file NetApp ONTAP memiliki dua tingkatan penyimpanan: penyimpanan primer dan penyimpanan kolam kapasitas. Penyimpanan primer disediakan, dapat diskalakan, penyimpanan SSD berkinerja tinggi yang dibuat khusus untuk bagian aktif kumpulan data Anda. Penyimpanan kolam kapasitas adalah tingkat penyimpanan yang sepenuhnya elastis yang dapat menskalakan hingga ukuran petabyte dan dioptimalkan biaya untuk data yang jarang diakses.

Data pada setiap volume secara otomatis berjenjang ke tingkat penyimpanan kumpulan kapasitas berdasarkan kebijakan tingkatan volume, periode pendinginan, dan pengaturan ambang batas. Bagian berikut menjelaskan kebijakan tingkatan ONTAP volume dan ambang batas yang digunakan untuk menentukan kapan data berjenjang ke kumpulan kapasitas.

Kebijakan tingkatan volume

Anda menentukan cara menggunakan FSx Anda untuk tingkatan penyimpanan sistem file ONTAP dengan memilih kebijakan tiering untuk setiap volume pada sistem file. Anda memilih kebijakan tiering saat membuat volume, dan Anda dapat memodifikasinya kapan saja dengan konsol Amazon FSx, API AWS CLI, atau NetApp menggunakan alat manajemen. Anda dapat memilih dari salah satu kebijakan berikut yang menentukan data mana, jika ada, yang berjenjang ke penyimpanan kumpulan kapasitas.

> **Note**
>
> Tiering dapat memindahkan data file dan data snapshot Anda ke tingkat kumpulan kapasitas. Namun, metadata file selalu tetap pada tingkat SSD. Untuk informasi selengkapnya, lihat Bagaimana penyimpanan SSD digunakan.

- Otomatis — Kebijakan ini memindahkan semua data dingin—data pengguna dan snapshot—ke tingkat kumpulan kapasitas. Tingkat pendinginan data ditentukan oleh periode pendinginan kebijakan, yang secara default adalah 31 hari, dan dapat dikonfigurasi ke nilai antara 2—183 hari. Ketika blok data dingin yang mendasarinya dibaca secara acak (seperti pada akses file biasa), mereka dibuat panas dan ditulis ke tingkat penyimpanan utama. Ketika blok data dingin dibaca secara berurutan (misalnya, dengan pemindaian antivirus), mereka tetap dingin dan tetap berada di tingkat penyimpanan kolam kapasitas. Ini adalah kebijakan default saat membuat volume menggunakan konsol Amazon FSx.
- Hanya Snapshot — Kebijakan ini hanya memindahkan data snapshot ke tingkat penyimpanan kumpulan kapasitas. Tingkat di mana snapshot berjenjang ke kumpulan kapasitas ditentukan oleh periode pendinginan kebijakan, yang secara default diatur ke 2 hari, dan dapat dikonfigurasi ke nilai antara 2—183 hari. Ketika data snapshot dingin dibaca, mereka dibuat panas dan ditulis ke tingkat penyimpanan utama. Ini adalah kebijakan default saat membuat volume menggunakan AWS CLI, Amazon FSx API, atau NetApp ONTAP CLI.
- Semua — Kebijakan ini menandai semua data pengguna dan data snapshot sebagai dingin, dan menyimpannya di tingkat kumpulan kapasitas. Ketika blok data dibaca, mereka tetap dingin dan tidak ditulis ke tingkat penyimpanan utama. Ketika data ditulis ke volume dengan kebijakan All tiering, awalnya masih ditulis ke tingkat penyimpanan SSD, dan berjenjang ke kumpulan kapasitas dengan proses latar belakang. Perhatikan bahwa metadata file selalu tetap pada tingkat SSD.
- Tidak ada — Kebijakan ini menyimpan semua data volume Anda di tingkat penyimpanan utama, dan mencegahnya dipindahkan ke penyimpanan kumpulan kapasitas. Jika Anda menetapkan volume ke kebijakan ini setelah menggunakan kebijakan lain, data yang ada dalam volume yang ada dalam penyimpanan kumpulan kapasitas dipindahkan ke penyimpanan SSD dengan proses latar belakang selama penggunaan SSD Anda di bawah 90%. Proses latar belakang ini dapat dipercepat dengan sengaja membaca data atau dengan memodifikasi kebijakan pengambilan cloud volume Anda. Untuk informasi selengkapnya, lihat Kebijakan pengambilan cloud.

Sebagai praktik terbaik, saat memigrasikan data yang Anda rencanakan untuk disimpan dalam jangka panjang dalam penyimpanan kumpulan kapasitas, sebaiknya gunakan kebijakan tingkatan Otomatis pada volume Anda. Dengan tiering Otomatis, data disimpan di tingkat penyimpanan SSD selama minimal 2 hari (berdasarkan periode pendinginan volume) sebelum dipindahkan ke tingkat kolam kapasitas. Mempertahankan data pada penyimpanan SSD setidaknya selama 2 hari memungkinkan ONTAP menjalankan penghematan kompresi dan deduplikasi pasca-proses pada data Anda, yang disimpan saat data berjenjang ke kumpulan kapasitas. ONTAP hanya menjalankan kompresi dan deduplikasi pasca-proses untuk data pada penyimpanan SSD, jadi memilih kebijakan ini dapat membantu Anda memaksimalkan penghematan penyimpanan jangka panjang Anda. Anda

juga dapat memaksimalkan kecepatan transfer cadangan pertama yang Anda buat dari volume Anda, karena data yang sedang dicadangkan ada di penyimpanan SSD.

Untuk informasi selengkapnya tentang menyetel atau memodifikasi kebijakan tingkatan volume, lihat. Menyetel kebijakan tingkatan volume

Periode pendinginan berjenjang

Periode pendinginan tingkat volume menetapkan jumlah waktu yang diperlukan untuk data di tingkat SSD ditandai sebagai dingin. Periode pendinginan berlaku untuk kebijakan `Auto` dan `Snapshot-only` tiering. Anda dapat mengatur periode pendinginan ke nilai dalam kisaran 2-183 hari. Untuk informasi lebih lanjut tentang pengaturan periode pendinginan, lihatMengatur hari pendinginan minimum.

Data berjenjang 24-48 jam setelah periode pendinginannya berakhir. Tiering adalah proses latar belakang yang mengkonsumsi sumber daya jaringan, dan memiliki prioritas lebih rendah daripada permintaan yang dihadapi klien. Aktivitas tingkatan dibatasi ketika ada permintaan yang dihadapi klien yang sedang berlangsung.

Kebijakan pengambilan cloud

Kebijakan pengambilan cloud volume menetapkan kondisi yang menentukan kapan data yang dibaca dari tingkat kumpulan kapasitas diizinkan untuk dipromosikan ke tingkat SSD. Jika kebijakan pengambilan cloud disetel ke apa pun selain`Default`, kebijakan ini akan mengesampingkan perilaku pengambilan kebijakan tiering volume Anda. Volume dapat memiliki salah satu kebijakan pengambilan cloud berikut:

- Default — Kebijakan ini mengambil data berjenjang berdasarkan kebijakan tiering yang mendasari volume. Ini adalah kebijakan pengambilan cloud default untuk semua volume.
- Tidak Pernah — Kebijakan ini tidak pernah mengambil data berjenjang, terlepas dari apakah pembacaannya berurutan atau acak. Ini mirip dengan menyetel kebijakan tiering volume Anda ke Semua, kecuali Anda dapat menggunakannya dengan kebijakan lain— Otomatis, Hanya Snapshot —ke data tingkat sesuai dengan periode pendinginan minimum, bukan segera.
- Saat dibaca — Kebijakan ini mengambil data berjenjang untuk semua pembacaan data berbasis klien. Kebijakan ini tidak berpengaruh saat menggunakan kebijakan All tiering.
- Promosikan — Kebijakan ini menandai semua data volume yang ada di kumpulan kapasitas untuk diambil ke tingkat SSD. Data ditandai saat berikutnya pemindai tingkat latar belakang harian berjalan. Kebijakan ini bermanfaat untuk aplikasi yang memiliki beban kerja siklus yang jarang

berjalan, tetapi memerlukan kinerja tingkat SSD saat dijalankan. Kebijakan ini tidak berpengaruh saat menggunakan kebijakan All tiering.

Untuk informasi tentang menyetel kebijakan pengambilan cloud volume, lihatMenyetel kebijakan pengambilan cloud volume.

Ambang batas jenjang

Pemanfaatan kapasitas penyimpanan SSD sistem file menentukan bagaimana ONTAP mengelola perilaku tiering untuk semua volume Anda. Berdasarkan penggunaan kapasitas penyimpanan SSD sistem file, ambang berikut menetapkan perilaku tiering seperti yang dijelaskan. Untuk informasi tentang cara memantau pemanfaatan kapasitas tingkat penyimpanan SSD volume, lihatMemantau kapasitas penyimpanan volume.

> **Note**
>
> Kami menyarankan agar Anda tidak melebihi 80% pemanfaatan kapasitas penyimpanan dari tingkat penyimpanan SSD Anda. Untuk sistem file scale-out, rekomendasi ini berlaku untuk pemanfaatan rata-rata total di semua agregat sistem file Anda dan untuk pemanfaatan masing-masing agregat individu. Ini memastikan bahwa tiering berfungsi dengan benar, dan menyediakan overhead untuk data baru. Jika tingkat penyimpanan SSD Anda secara konsisten di atas pemanfaatan kapasitas penyimpanan 80%, Anda dapat meningkatkan kapasitas tingkat penyimpanan SSD Anda. Untuk informasi selengkapnya, lihat Memperbarui penyimpanan SSD sistem file dan IOPS.

FSx untuk ONTAP menggunakan ambang kapasitas penyimpanan berikut untuk mengelola tiering volume:

- <= 50% pemanfaatan tingkat penyimpanan SSD — Pada ambang batas ini, tingkat penyimpanan SSD dianggap kurang dimanfaatkan, dan hanya volume yang menggunakan kebijakan All tiering yang memiliki data berjenjang ke penyimpanan kolam kapasitas. Volume dengan kebijakan Otomatis dan khusus Snapshot tidak membuat data peringkat pada ambang batas ini.
- > Pemanfaatan tingkat penyimpanan SSD 50% — Volume dengan data tingkat kebijakan tiering Otomatis dan Snapshot saja berdasarkan pengaturan hari pendinginan minimum tiering. Pengaturan default adalah 31 hari.

- > = 90% pemanfaatan tingkat penyimpanan SSD — Pada ambang batas ini, Amazon FSx memprioritaskan pelestarian ruang di tingkat penyimpanan SSD. Data dingin dari tingkat kumpulan kapasitas tidak lagi dipindahkan ke tingkat penyimpanan SSD saat dibaca untuk volume menggunakan kebijakan Auto dan Snapshot saja.
- > = 98% Pemanfaatan tingkat penyimpanan SSD — Semua fungsionalitas tiering berhenti ketika tingkat penyimpanan SSD berada pada atau di atas 98% pemanfaatan. Anda dapat terus membaca dari tingkatan penyimpanan, tetapi Anda tidak dapat menulis ke tingkatan.

Snapshot dan kapasitas penyimpanan volume

Snapshot adalah gambar hanya-baca dari Amazon FSx untuk volume NetApp ONTAP pada suatu titik waktu. Snapshot menawarkan perlindungan terhadap penghapusan atau modifikasi file yang tidak disengaja dalam volume Anda. Dengan snapshot, pengguna Anda dapat dengan mudah melihat dan memulihkan file atau folder individual dari snapshot sebelumnya.

Snapshot disimpan di samping data sistem file Anda, dan mereka menghabiskan kapasitas penyimpanan sistem file. Namun, snapshot mengkonsumsi kapasitas penyimpanan hanya untuk bagian file yang berubah sejak snapshot terakhir. Snapshot tidak disertakan dalam backup volume sistem file Anda.

Snapshot diaktifkan secara default pada volume Anda, menggunakan kebijakan snapshot default. Snapshot disimpan di `.snapshot` direktori di root volume. Anda dapat mengelola kapasitas penyimpanan volume untuk snapshot dengan cara berikut:

- Kebijakan snapshot — Pilih kebijakan snapshot bawaan atau pilih kebijakan khusus yang Anda buat di ONTAP CLI atau REST API.
- Hapus snapshot secara manual - Dapatkan kembali kapasitas penyimpanan dengan menghapus snapshot secara manual.
- Buat kebijakan penghapusan otomatis snapshot — Buat kebijakan yang menghapus lebih banyak snapshot daripada kebijakan snapshot default.
- Matikan snapshot otomatis — Hemat kapasitas penyimpanan dengan mematikan snapshot otomatis.

Untuk informasi selengkapnya, lihat Cara menggunakan snapshot.

Kapasitas file volume

Amazon FSx untuk volume NetApp ONTAP memiliki pointer file yang digunakan untuk menyimpan metadata file seperti nama file, waktu terakhir diakses, izin, ukuran, dan untuk berfungsi sebagai petunjuk ke blok data. Pointer file ini disebut inode, dan setiap volume memiliki kapasitas terbatas untuk jumlah inode, yang disebut kapasitas file volume. Ketika volume berjalan rendah atau kehabisan file yang tersedia (inode), Anda tidak dapat menulis data tambahan ke volume itu.

Jumlah objek sistem file — file, direktori, salinan Snapshot — volume dapat berisi ditentukan oleh berapa banyak inode yang dimilikinya. Jumlah inode dalam volume meningkat sepadan dengan kapasitas penyimpanan volume (dan jumlah konstituen volume untuk volume). FlexGroup Secara default, FlexVol volume (atau FlexGroup konstituen) dengan kapasitas penyimpanan 648 GiB atau lebih semuanya memiliki jumlah inode yang sama: 21.251.126. Jika Anda membuat volume lebih besar dari 648 GiB dan Anda ingin memiliki lebih dari 21.251.126 inode, Anda harus meningkatkan jumlah maksimum inode (file) secara manual. Untuk informasi selengkapnya tentang melihat jumlah maksimum file untuk volume, lihatMelihat kapasitas file volume.

Jumlah default inode pada volume adalah 1 inode untuk setiap 32 KiB kapasitas penyimpanan volume, hingga ukuran volume 648 GiB. Untuk volume 1 GiB:

Volume_size_in_bytes × (1 file ÷ inode_size_in_bytes) = maksimum_number_of_files

1.073.741.824 byte × (1 file ÷ 32.768 byte) = 32.768 file

Anda dapat meningkatkan jumlah maksimum inode yang dapat dikandung volume, hingga maksimum 1 inode untuk setiap 4 KiB kapasitas penyimpanan. Untuk volume 1 GiB. ini meningkatkan jumlah maksimum inode atau file dari 32.768 menjadi 262.144:

1.073.741.824 byte × (1 file ÷ 4096 byte) = 262.144 file

FSx untuk volume ONTAP dapat memiliki maksimum 2 miliar inode.

Untuk informasi tentang mengubah jumlah maksimum file yang dapat disimpan volume, lihatMeningkatkan jumlah maksimum file pada volume.

Memperbarui kapasitas penyimpanan volume

Anda dapat mengelola kapasitas penyimpanan volume dengan menambah atau mengurangi ukuran volume secara manual menggunakan AWS Management Console, AWS CLI dan API, dan CLI

ONTAP. Anda juga dapat mengaktifkan autosizing volume sehingga ukuran volume secara otomatis tumbuh atau menyusut ketika mencapai ambang batas kapasitas penyimpanan bekas tertentu. Anda menggunakan CLI ONTAP untuk mengelola autosizing volume.

Untuk mengubah kapasitas penyimpanan volume (konsol)

- Anda dapat menambah atau mengurangi kapasitas penyimpanan volume menggunakan konsol Amazon FSx, AWS CLI, dan API. Untuk informasi selengkapnya, lihat Memperbarui volume.

Anda juga dapat menggunakan ONTAP CLI untuk memodifikasi kapasitas penyimpanan volume menggunakan perintah. `volume modify`

Untuk mengubah ukuran volume (ONTAP CLI)

1. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen Amazon fsX NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *`management_endpoint_ip`* dengan alamat IP port manajemen sistem file.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Untuk informasi selengkapnya, lihat Mengelola sistem file dengan ONTAP CLI.
2. Gunakan perintah volume modify ONTAP CLI untuk memodifikasi kapasitas penyimpanan volume. Jalankan perintah berikut, menggunakan data Anda sebagai pengganti nilai-nilai berikut:

   - Ganti *`svm_name`*dengan nama mesin virtual penyimpanan (SVM) tempat volume dibuat.
   - Ganti *`vol_name`*dengan nama volume yang ingin Anda ubah ukurannya.
   - Ganti *`vol_size`*dengan ukuran volume baru dalam format *`integer`*`[KB|MB|GB|TB|PB]`; misalnya, `100GB` untuk meningkatkan ukuran volume menjadi 100 gigabyte.

   ```
   ::> volume modify -vserver svm_name -volume vol_name -size vol_size
   ```

Mengaktifkan autosizing volume

Volume autosizing sehingga volume akan secara otomatis tumbuh ke ukuran tertentu ketika mencapai ambang ruang yang digunakan. Anda dapat melakukan ini untuk tipe FlexVol volume (tipe volume default untuk FSx untuk ONTAP) menggunakan perintah ONTAP `volume autosize`CLI.

Untuk mengaktifkan autosizing volume (ONTAP CLI)

1. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen Amazon fsX NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Untuk informasi selengkapnya, lihat Mengelola sistem file dengan ONTAP CLI.

2. Gunakan `volume autosize` perintah seperti yang ditunjukkan, menggantikan nilai-nilai berikut:

   - Ganti *svm_name*dengan nama SVM tempat volume dibuat.
   - Ganti *vol_name*dengan nama volume yang ingin Anda ubah ukurannya.
   - Ganti *grow_threshold*dengan nilai persentase spasi yang digunakan (seperti`90`) di mana volume akan secara otomatis meningkat dalam ukuran (hingga *max_size*nilai).
   - Ganti *max_size*dengan ukuran maksimum yang volumenya bisa bertambah. Gunakan format *integer*`[KB|MB|GB|TB|PB]`; misalnya,`300TB`. Ukuran maksimumnya adalah 300 TB. Defaultnya adalah 120% dari ukuran volume.
   - Ganti *min_size* dengan ukuran minimum yang volume akan menyusut. Gunakan format yang sama seperti untuk *max_size*.
   - Ganti *shrink_threshold* dengan persentase spasi yang digunakan di mana volume akan secara otomatis menyusut dalam ukuran.

   ```
   ::> volume autosize -vserver svm_name -volume vol_name -mode grow_shrink -
   grow-threshold-percent grow_threshold -maximum-size max_size -shrink-threshold-
   percent shrink_threshold -minimum-size min_size
   ```

Memantau kapasitas penyimpanan volume

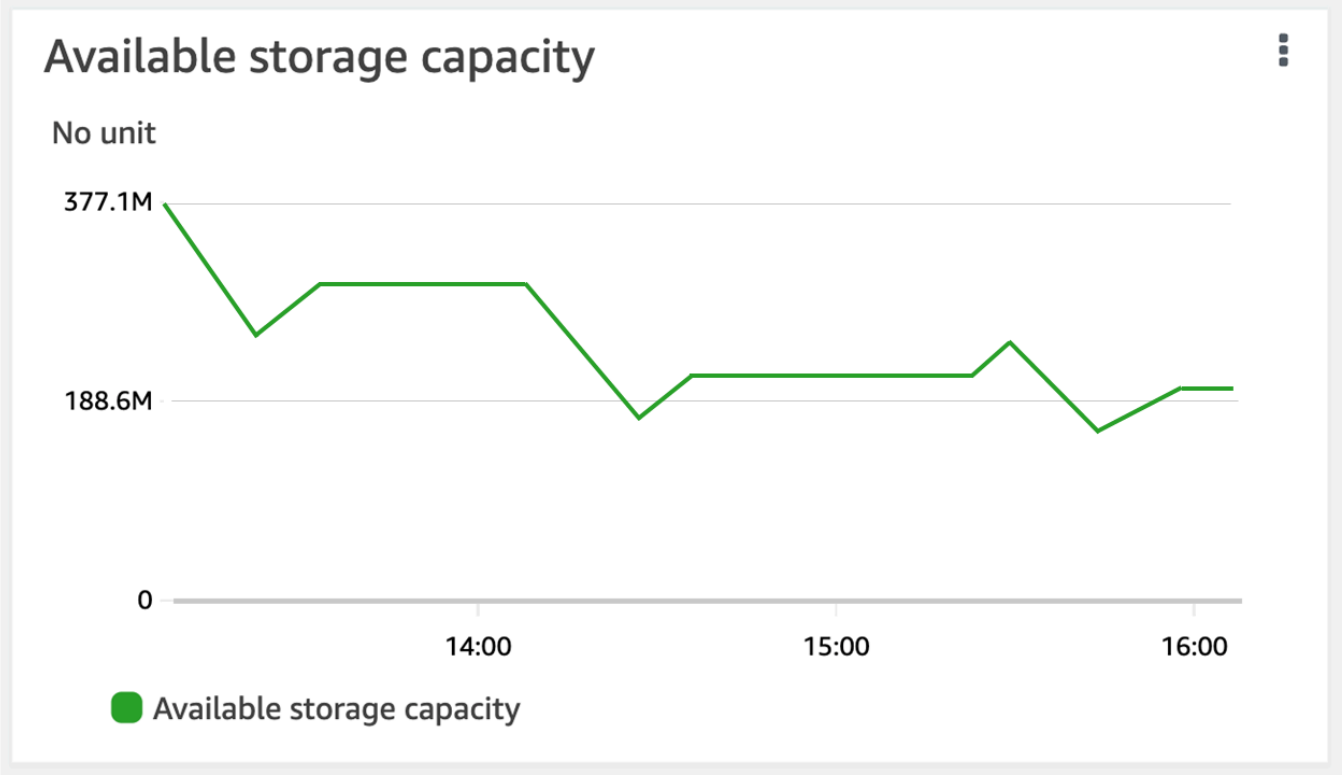
Anda dapat melihat penyimpanan volume yang tersedia dan distribusi penyimpanannya di AWS Management Console, AWS CLI, dan CLI NetApp ONTAP.

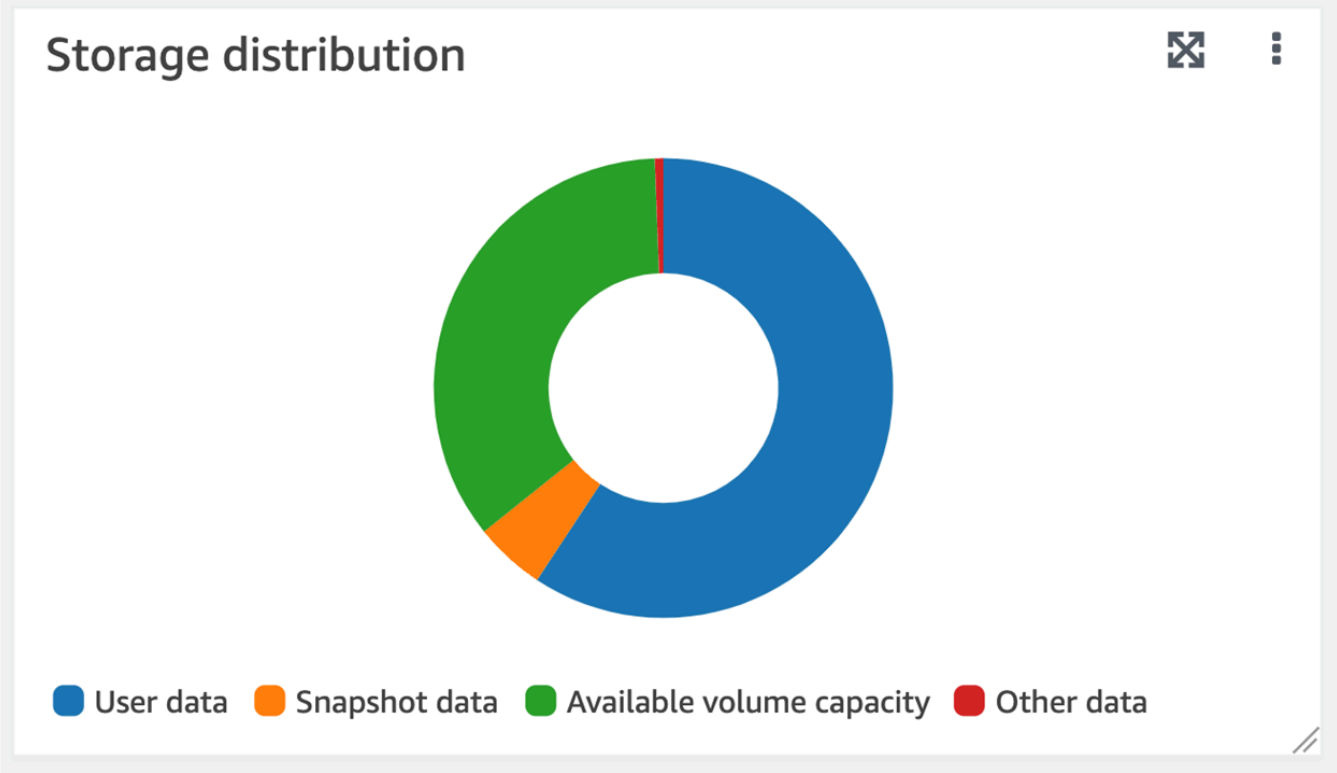
Untuk memantau kapasitas penyimpanan volume (konsol)

Grafik penyimpanan yang tersedia menampilkan jumlah kapasitas penyimpanan gratis pada volume dari waktu ke waktu. Grafik distribusi Storage menunjukkan bagaimana kapasitas penyimpanan volume saat ini didistribusikan pada 4 kategori:

- Data pengguna
- Data snapshot
- Kapasitas volume yang tersedia
- Data lainnya

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Pilih Volume di kolom navigasi kiri, lalu pilih volume ONTAP yang ingin Anda lihat informasi kapasitas penyimpanan. Halaman detail volume muncul.
3. Di panel kedua, pilih tab Monitoring. Grafik distribusi Penyimpanan dan Penyimpanan yang Tersedia ditampilkan, bersama dengan beberapa grafik lainnya.





Untuk memantau kapasitas penyimpanan volume (ONTAPCLI)

Anda dapat memantau bagaimana kapasitas penyimpanan volume Anda dikonsumsi dengan menggunakan perintah `volume show-space` ONTAP CLI. Untuk informasi selengkapnya, lihat `volume show-space`di Pusat NetApp ONTAP Dokumentasi.

1. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen Amazon fsX NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *`management_endpoint_ip`* dengan alamat IP port manajemen sistem file.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Untuk informasi selengkapnya, lihat Mengelola sistem file dengan ONTAP CLI.

2. Lihat penggunaan kapasitas penyimpanan volume dengan mengeluarkan perintah berikut, mengganti nilai berikut:

   - Ganti *`svm_name`*dengan nama SVM tempat volume dibuat.
   - Ganti *`vol_name`*dengan nama volume yang Anda setel kebijakan data-tiering.

```
::> volume show-space -vserver svm_name -volume vol_name
```

Jika perintah berhasil, Anda akan melihat output yang mirip dengan berikut ini:

```
Vserver : svm_name
Volume  : vol_name
Feature                                     Used      Used%
--------------------------------     ----------     ------
User Data                                140KB         0%
Filesystem Metadata                    164.4MB         1%
Inodes                                 10.28MB         0%
Snapshot Reserve                       563.2MB         5%
Deduplication                             12KB         0%
Snapshot Spill                          9.31GB        85%
Performance Metadata                     668KB         0%

Total Used                             10.03GB        91%

Total Physical Used                    10.03GB        91%
```

Output dari perintah ini menunjukkan jumlah ruang fisik yang ditempati berbagai jenis data pada volume ini. Ini juga menunjukkan persentase kapasitas total volume yang dikonsumsi setiap jenis data. Dalam contoh ini, `Snapshot Spill` dan `Snapshot Reserve` mengkonsumsi gabungan 90 persen dari kapasitas volume.

`Snapshot Reserve`menunjukkan jumlah ruang disk yang disediakan untuk menyimpan salinan Snapshot. Jika penyimpanan salinan Snapshot melebihi ruang cadangan, itu tumpah ke sistem file dan jumlah ini ditampilkan di bawah. `Snapshot Spill`

Untuk menambah jumlah ruang yang tersedia, Anda dapat meningkatkan ukuran volume, atau Anda dapat menghapus snapshot yang tidak Anda gunakan, seperti yang ditunjukkan dalam prosedur berikut.

Untuk jenis FlexVol volume (tipe volume default untuk FSx untuk volume ONTAP), Anda juga dapat mengaktifkan autosizing volume. Saat Anda mengaktifkan autosizing, ukuran volume secara otomatis meningkat ketika mencapai ambang batas tertentu. Anda juga dapat menonaktifkan snapshot otomatis. Kedua fitur ini dijelaskan di bagian berikut.

Menyetel kebijakan tingkatan volume

Anda dapat mengubah kebijakan tingkatan volume menggunakan AWS Management Console, AWS CLI dan API, dan CLI ONTAP.

Untuk mengubah kebijakan tingkatan data volume (konsol)

Gunakan prosedur berikut untuk memodifikasi kebijakan tingkat data volume menggunakan. AWS Management Console

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Pilih Volume di panel navigasi kiri, lalu pilih volume ONTAP yang ingin Anda ubah kebijakan tingkat data.
3. Pilih Perbarui volume dari menu tarik-turun Tindakan. Jendela Perbarui volume muncul.
4. Untuk kebijakan tingkatan kumpulan Kapasitas, pilih kebijakan baru untuk volume. Untuk informasi selengkapnya, lihat Kebijakan tingkatan volume.
5. Pilih Perbarui untuk menerapkan kebijakan baru ke volume.

Untuk menetapkan kebijakan tingkatan volume (CLI)

- Ubah kebijakan tiering volume menggunakan perintah CLI update-volume (adalah tindakan API Amazon UpdateVolumeFSx yang setara). Contoh perintah CLI berikut menetapkan kebijakan tingkat data volume ke. SNAPSHOT_ONLY

```
aws fsx update-volume \
    --volume-id fsxvol-abcde0123456789f
    --ontap-configuration TieringPolicy={Name=SNAPSHOT_ONLY}
```

Untuk permintaan yang berhasil, sistem merespons dengan deskripsi volume.

```
{
    "Volume": {
        "CreationTime": "2021-10-05T14:27:44.332000-04:00",
        "FileSystemId": "fs-abcde0123456789f",
        "Lifecycle": "CREATED",
        "Name": "vol1",
        "OntapConfiguration": {
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
```

```
            "SecurityStyle": "UNIX",
            "SizeInMegabytes": 1048576,
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abc0123de456789f",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "CoolingPeriod": 2,
                "Name": "SNAPSHOT_ONLY"
            },
            "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcde0123456789f/fsvol-abc012def3456789a",
        "VolumeId": "fsvol-abc012def3456789a",
        "VolumeType": "ONTAP"
    }
}
```

Untuk mengubah kebijakan tingkatan volume (ONTAP CLI)

Anda menggunakan perintah `volume modify` ONTAP CLI untuk menyetel kebijakan tiering volume. Untuk informasi selengkapnya, lihat `volume modify`di Pusat Dokumentasi NetApp ONTAP.

1. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen Amazon fsX NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *`management_endpoint_ip`* dengan alamat IP port manajemen sistem file.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Untuk informasi selengkapnya, lihat Mengelola sistem file dengan ONTAP CLI.

2. Masukkan mode lanjutan CLI ONTAP menggunakan perintah berikut.

   ```
   FSx::> set adv

   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. Gunakan perintah berikut untuk mengubah kebijakan tingkat data volume, menggantikan nilai berikut:

   - Ganti *svm_name*dengan nama SVM tempat volume dibuat.
   - Ganti *vol_name*dengan nama volume yang Anda setel kebijakan data-tiering.
   - Ganti *tiering_policy*dengan kebijakan yang diinginkan. Nilai yang valid adalah `snapshot-only`, `auto`, `all`, atau `none`. Untuk informasi selengkapnya, lihat Kebijakan tingkatan volume.

```
FSx::> volume modify -vserver svm_name -volume vol_name -tiering-
policy tiering_policy
```

Mengatur hari pendinginan minimum

Hari pendinginan minimum untuk volume mengatur ambang batas yang digunakan untuk menentukan data mana yang hangat dan data mana yang dingin. Anda dapat mengatur hari pendinginan minimum volume menggunakan AWS CLI dan API, dan CLI ONTAP.

Untuk mengatur hari pendinginan minimum volume (CLI)

- Ubah konfigurasi volume dengan menggunakan perintah CLI update-volume (UpdateVolumeadalah tindakan API Amazon fsX yang setara). Contoh perintah CLI berikut menetapkan volume `CoolingPeriod` untuk 104 hari.

```
aws fsx update-volume \
    --volume-id fsxvol-abcde0123456789f
    --ontap-configuration TieringPolicy={Name=SNAPSHOT_ONLY}
aws fsx update-volume --volume-id fsvol-006530558c14224ac --ontap-configuration
 TieringPolicy={CoolingPeriod=104}
```

  Sistem merespons dengan deskripsi volume untuk permintaan yang berhasil.

```
{
    "Volume": {
        "CreationTime": "2021-10-05T14:27:44.332000-04:00",
        "FileSystemId": "fs-abcde0123456789f",
        "Lifecycle": "CREATED",
```

```
        "Name": "vol1",
        "OntapConfiguration": {
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "UNIX",
            "SizeInMegabytes": 1048576,
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abc0123de456789f",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "CoolingPeriod": 104,
                "Name": "SNAPSHOT_ONLY"
            },
            "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcde0123456789f/fsvol-abc012def3456789a",
        "VolumeId": "fsvol-abc012def3456789a",
        "VolumeType": "ONTAP"
    }
}
```

Untuk mengatur hari pendinginan minimum volume (ONTAP CLI)

Gunakan perintah `volume modify` ONTAP CLI untuk mengatur jumlah minimum hari pendinginan untuk volume yang ada. Untuk informasi selengkapnya, lihat `volume modify`di Pusat Dokumentasi NetApp ONTAP.

1. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen Amazon fsX NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *`management_endpoint_ip`* dengan alamat IP port manajemen sistem file.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Untuk informasi selengkapnya, lihat Mengelola sistem file dengan ONTAP CLI.

2. Masukkan mode lanjutan CLI ONTAP menggunakan perintah berikut.

   ```
   FSx::> set adv
   ```

```
Warning: These advanced commands are potentially dangerous; use them only when
     directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y
```

3. Gunakan perintah berikut untuk mengubah hari pendinginan minimum tingkat volume Anda, menggantikan nilai-nilai berikut:

   - Ganti *svm_name*dengan nama SVM tempat volume dibuat.
   - Ganti *vol_name*dengan nama volume yang Anda atur hari pendinginan.
   - Ganti *cooling_days* dengan yang diinginkan, bilangan bulat antara 2-183.

   ```
   FSx::> volume modify -vserver svm_name -volume vol_name -tiering-minimum-cooling-
   days cooling_days
   ```

   Sistem merespons sebagai berikut untuk permintaan yang berhasil.

   ```
   Volume modify successful on volume vol_name of Vserver svm_name.
   ```

Menyetel kebijakan pengambilan cloud volume

Gunakan perintah `volume modify` ONTAP CLI untuk menyetel kebijakan pengambilan cloud untuk volume yang ada. Untuk informasi selengkapnya, lihat `volume modify`di Pusat Dokumentasi NetApp ONTAP.

Untuk menyetel kebijakan pengambilan cloud volume (ONTAP CLI)

1. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen Amazon fsX NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Untuk informasi selengkapnya, lihat Mengelola sistem file dengan ONTAP CLI.

2. Masukkan mode lanjutan CLI ONTAP menggunakan perintah berikut.

   ```
   FSx::> set adv
   ```

```
Warning: These advanced commands are potentially dangerous; use them only when
     directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y
```

3. Gunakan perintah berikut untuk menyetel kebijakan pengambilan cloud volume, menggantikan nilai berikut:

   - Ganti *svm_name*dengan nama SVM tempat volume dibuat.
   - Ganti *vol_name*dengan nama volume yang Anda setel kebijakan pengambilan cloud.
   - Ganti *retrieval_policy* dengan nilai yang diinginkan, baik`default`,`on-read`,`never`, atau`promote`.

   ```
   FSx::> volume modify -vserver svm_name -volume vol_name -cloud-retrieval-
   policy retrieval_policy
   ```

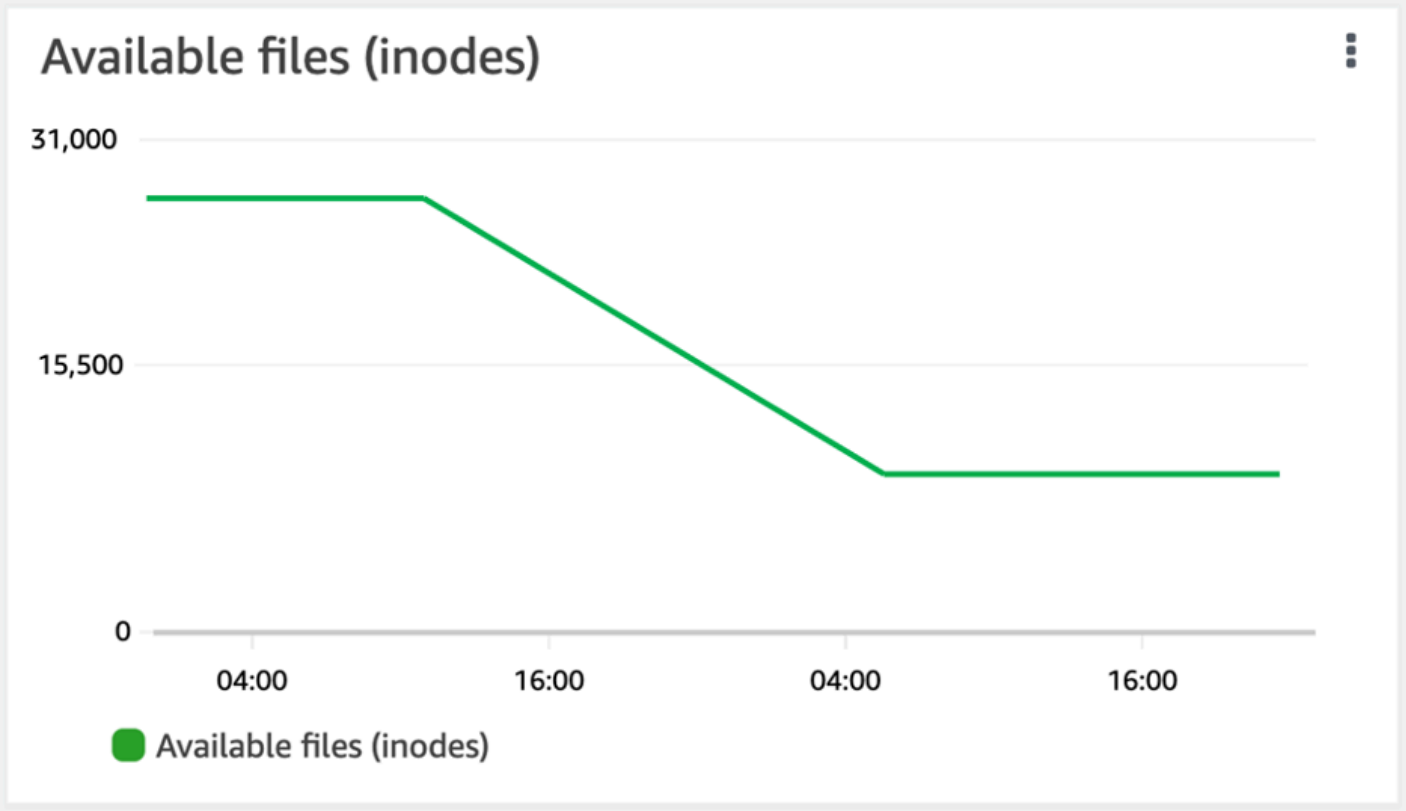
   Sistem merespons sebagai berikut untuk permintaan yang berhasil.

   ```
   Volume modify successful on volume vol_name of Vserver svm_name.
   ```

Melihat kapasitas file volume

Anda dapat menggunakan salah satu metode berikut untuk melihat jumlah maksimum file yang diizinkan dan jumlah file yang sudah digunakan pada volume.

- Metrik CloudWatch volume `FilesCapacity` dan`FilesUsed`.
- Di konsol Amazon FSx, navigasikan ke bagan File yang tersedia (inode) di tab Pemantauan volume Anda. Gambar berikut menunjukkan file yang tersedia (inode) pada volume menurun dari waktu ke waktu.



Meningkatkan jumlah maksimum file pada volume

FSx untuk volume ONTAP dapat kehabisan kapasitas file ketika jumlah inode yang tersedia, atau pointer file, habis.

Untuk meningkatkan jumlah maksimum file pada volume (ONTAPCLI)

Anda menggunakan perintah `volume modify` ONTAP CLI untuk meningkatkan jumlah maksimum file pada volume. Untuk informasi selengkapnya, lihat `volume modify`di Pusat NetApp ONTAP Dokumentasi.

1. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen Amazon fsX NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *`management_endpoint_ip`* dengan alamat IP port manajemen sistem file.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Untuk informasi selengkapnya, lihat Mengelola sistem file dengan ONTAP CLI.

2. Lakukan salah satu langkah berikut sesuai dengan kasus penggunaan Anda. Ganti *svm_name*dan *vol_name*dengan nilai-nilai Anda.

   - Untuk mengonfigurasi volume agar selalu memiliki jumlah maksimum file (inode) yang tersedia, lakukan hal berikut:

     1. Masuk ke mode lanjutan di CLI ONTAP dengan menggunakan perintah berikut.

        ```
        ::> set adv
        ```

     2. Setelah menjalankan perintah ini, Anda akan melihat output ini. Masuk y untuk melanjutkan.

        ```
        Warning: These advanced commands are potentially dangerous; use them only
         when
        directed to do so by NetApp personnel.
        Do you want to continue? {y|n}: y
        ```

     3. Masukkan perintah berikut untuk selalu menggunakan jumlah maksimum file pada volume:

        ```
        ::> volume modify -vserver svm_name -volume vol_name -files-set-maximum true
        ```

   - Untuk secara manual menentukan jumlah total file yang diizinkan pada volume*max_number_files* = (current_size_of_volume) × (1 file ÷ 4 KiB), dengan, hingga nilai maksimum yang mungkin 2 miliar, gunakan perintah berikut:

     ```
     ::> volume modify -vserver svm_name -volume vol_name -files max_number_files
     ```

Mengaktifkan mode tulis cloud volume

Gunakan perintah `volume modify` ONTAP CLI untuk mengaktifkan atau menonaktifkan mode tulis cloud untuk volume yang ada. Untuk informasi selengkapnya, lihat `volume modify`di Pusat Dokumentasi NetApp ONTAP.

Prasyarat untuk mengatur mode tulis cloud adalah:

- Volume harus berupa volume yang ada. Anda hanya dapat mengaktifkan fitur pada volume yang ada.

- Volume harus berupa volume baca-tulis (RW).
- Volume harus memiliki kebijakan All tiering. Untuk informasi selengkapnya tentang memodifikasi kebijakan tingkatan volume, lihat. Menyetel kebijakan tingkatan volume

Mode tulis cloud sangat membantu untuk kasus-kasus seperti migrasi, misalnya, di mana sejumlah besar data ditransfer ke sistem file menggunakan protokol NFS.

Untuk mengatur mode tulis cloud volume (ONTAP CLI)

1. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen Amazon fsX NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Untuk informasi selengkapnya, lihat Mengelola sistem file dengan ONTAP CLI.
2. Masukkan mode lanjutan CLI ONTAP menggunakan perintah berikut.

   ```
   FSx::> set -privilege advanced
   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```
3. Gunakan perintah berikut untuk mengatur mode tulis cloud volume, menggantikan nilai berikut:

   - Ganti *svm_name*dengan nama SVM tempat volume dibuat.
   - Ganti *vol_name*dengan nama volume yang Anda atur mode tulis cloud.
   - Ganti *vol_cw_mode* dengan salah satu `true` untuk mengaktifkan mode tulis cloud pada volume atau `false` untuk menonaktifkannya.

   ```
   FSx::> volume modify -vserver svm_name -volume vol_name -is-cloud-write-
   enabled vol_cw_mode
   ```

   Sistem merespons sebagai berikut untuk permintaan yang berhasil.

   ```
   Volume modify successful on volume vol_name of Vserver svm_name.
   ```

Melindungi data Anda

Di luar mereplikasi data sistem file Anda secara otomatis untuk menjamin daya tahan tinggi, Amazon FSx memberi Anda pilihan berikut untuk lebih melindungi data yang tersimpan pada sistem file Anda:

- Backup asli Amazon FSx mendukung retensi cadangan dan kebutuhan kepatuhan Anda dalam Amazon FSx. Anda juga dapat menggunakannya AWS Backup untuk mengelola, mengotomatisasi, dan melindungi cadangan Anda secara terpusat di Layanan AWS cloud.
- Snapshots memungkinkan pengguna Anda untuk dengan mudah membatalkan perubahan file dan membandingkan versi file dengan memulihkan file ke versi sebelumnya.
- Replikasi sistem file Amazon FSx Anda ke sistem file kedua untuk memberikan perlindungan dan pemulihan data. Replikasi, ketika diaktifkan, terjadi secara otomatis, terjadwal.
- SnapLockdapat melindungi file Anda dengan mentransisisinya ke status tulis sekali, baca banyak (WORM), yang mencegah modifikasi atau penghapusan untuk periode retensi tertentu.

Topik

Menggunakan cadangan

Dengan FSx untuk ONTAP, Anda dapat mengambil backup harian otomatis dan backup volume yang diprakarsai pengguna pada sistem file Anda. FSx untuk cadangan ONTAP adalah per volume, sehingga setiap cadangan hanya berisi data dalam volume tertentu. Cadangan Amazon FSx sangat tahan lama dan inkremental.

Semua backup Amazon FSx (backup harian otomatis dan backup yang diprakarsai pengguna) bersifat inkremental. Ini berarti bahwa hanya data pada volume yang telah berubah setelah cadangan terbaru Anda disimpan. Ini meminimalkan waktu yang diperlukan untuk membuat cadangan dan penyimpanan yang diperlukan untuk cadangan, yang menghemat biaya penyimpanan dengan tidak menduplikasi data. Saat Anda menghapus sebuah cadangan, hanya data yang unik dari cadangan tersebut yang dihapus. Setiap cadangan Amazon FSx berisi semua informasi yang diperlukan untuk

membuat volume baru dari cadangan, secara efektif memulihkan point-in-time snapshot dari volume sistem file.

Membuat cadangan rutin untuk volume Anda adalah praktik terbaik yang membantu mendukung retensi data dan kebutuhan kepatuhan Anda. Bekerja dengan cadangan Amazon FSx itu mudah, apakah itu membuat cadangan, memulihkan dari cadangan, atau menghapus cadangan.

Amazon FSx mendukung backup ONTAP FlexVol volume (pada semua sistem file) dan FlexGroup volume dengan `RW` (baca-tulis`OntapVolumeType`).

> **Note**
>
> Amazon FSx tidak mendukung pencadangan volume perlindungan data (DP), volume pembagian beban (LS), atau volume tujuan. FlexCache

Ada batasan jumlah cadangan yang dapat Anda simpan per sistem file dan per volume. Lihat informasi yang lebih lengkap di Kuota yang dapat Anda tingkatkan dan Kuota sumber daya untuk setiap sistem file.

Topik

Cara kerja backup

Cadangan Amazon FSx menggunakan snapshot - point-in-time, gambar hanya-baca volume Anda - untuk mempertahankan peningkatan antar cadangan. Setiap kali cadangan diambil, Amazon FSx pertama-tama mengambil snapshot volume Anda. Snapshot cadangan disimpan dalam volume Anda, dan menghabiskan ruang pada tingkat penyimpanan SSD Anda. Amazon FSx kemudian membandingkan snapshot ini dengan snapshot cadangan sebelumnya (jika ada) dan hanya menyalin data yang diubah ke cadangan Anda.

Jika tidak ada snapshot cadangan sebelumnya, maka seluruh konten snapshot cadangan terbaru disalin ke cadangan Anda. Setelah snapshot cadangan terbaru berhasil diambil, Amazon FSx menghapus snapshot cadangan sebelumnya. Snapshot yang digunakan untuk cadangan terbaru tetap ada di volume Anda hingga cadangan berikutnya diambil, saat proses berulang. Untuk mengoptimalkan biaya penyimpanan cadangan, ONTAP menjaga penghematan efisiensi penyimpanan volume dalam cadangannya.

Amazon FSx tidak dapat mencadangkan volume yang offline.

Persyaratan penyimpanan

Untuk mengambil cadangan volume Anda, volume dan sistem file Anda harus memiliki kapasitas penyimpanan SSD yang cukup untuk menyimpan snapshot cadangan. Saat mengambil snapshot cadangan, kapasitas penyimpanan tambahan yang dikonsumsi oleh snapshot tidak dapat menyebabkan volume melebihi 98% pemanfaatan penyimpanan SSD. Jika ini terjadi, cadangan akan gagal. Anda dapat meningkatkan penyimpanan SSD volume atau sistem file kapan saja untuk memastikan bahwa cadangan Anda tidak akan terganggu.

Bekerja dengan backup harian otomatis

Pencadangan harian otomatis volume sistem file Anda diaktifkan secara default saat Anda membuat sistem file. Anda dapat mengaktifkan atau menonaktifkan backup harian otomatis untuk sistem file kapan saja. Pencadangan harian otomatis terjadi selama jendela pencadangan harian, yang secara otomatis diatur saat Anda membuat sistem file. Anda dapat memodifikasi jendela cadangan harian kapan saja. Kami menyarankan Anda memilih waktu dalam sehari untuk pencadangan harian Anda yang berada di luar jam operasi normal untuk aplikasi yang menggunakan volume Anda untuk kinerja pencadangan yang lebih baik. Untuk informasi selengkapnya, lihat Backup dan pulihkan kinerja.

Anda dapat mengatur periode retensi untuk pencadangan harian otomatis menjadi antara 1 dan 90 hari di konsol saat membuat sistem file atau kapan saja. Periode retensi cadangan harian otomatis

default adalah 30 hari. Layanan menghapus cadangan harian otomatis setelah periode retensi berakhir. Menggunakan CLI atau API Anda dapat mengatur periode retensi menjadi antara 0 dan 90 hari; menyetelnya ke 0 mematikan pencadangan harian otomatis.

Jendela cadangan harian dan periode retensi cadangan adalah pengaturan tingkat sistem file yang berlaku untuk semua volume pada sistem file Anda. Anda dapat menggunakan konsol Amazon FSx AWS CLI, atau API untuk mengubah jendela cadangan dan periode penyimpanan cadangan untuk sistem file Anda, dan untuk mengaktifkan atau menonaktifkan pencadangan harian otomatis. Untuk informasi selengkapnya, lihat Memperbarui sistem file.

Anda tidak dapat membuat cadangan volume jika volumenya offline. Untuk informasi selengkapnya, lihat Cadangan dan volume offline.

> **Note**
>
> Pencadangan harian otomatis memiliki periode retensi maksimum 90 hari, tetapi pencadangan yang dimulai pengguna yang Anda buat, yang mencakup cadangan yang dibuat menggunakan AWS Backup, dipertahankan selamanya kecuali Anda atau layanan menghapusnya. AWS Backup

Anda dapat menghapus cadangan harian otomatis secara manual menggunakan konsol, CLI, dan API. Saat Anda menghapus volume, Anda juga menghapus cadangan harian otomatis untuk volume itu. Amazon FSx menyediakan opsi untuk membuat cadangan akhir volume sebelum Anda menghapusnya. Cadangan akhir disimpan selamanya, kecuali Anda menghapusnya. untuk informasi lebih lanjut, lihatMenghapus cadangan.

Bekerja dengan backup yang diinisiasi pengguna

Dengan Amazon FSx, Anda dapat secara manual mengambil cadangan volume sistem file Anda kapan saja menggunakan AWS Management Console,, AWS CLI dan API. Pencadangan yang diprakarsai pengguna Anda bersifat inkremental relatif terhadap cadangan lain yang mungkin telah dibuat untuk volume dan dipertahankan selamanya, kecuali jika Anda menghapusnya. Pencadangan yang diprakarsai pengguna dipertahankan bahkan setelah Anda menghapus volume atau sistem file tempat cadangan dibuat. Anda dapat menghapus backup yang diinisiasi pengguna hanya dengan menggunakan konsol, API, atau CLI Amazon FSx. Backup tidak pernah dihapus secara otomatis oleh Amazon FSx. Untuk informasi selengkapnya, lihat Menghapus cadangan.

Anda tidak dapat membuat cadangan volume jika volumenya offline. Untuk informasi selengkapnya, lihat Cadangan dan volume offline.

Menyalin tag ke cadangan

Saat Anda membuat atau memperbarui volume menggunakan CLI atau API, Anda dapat mengaktifkan `CopyTagsToBackups` untuk secara otomatis menyalin tag apa pun pada volume Anda ke cadangannya. Namun, jika Anda menambahkan tag apa pun saat membuat cadangan yang dimulai pengguna, termasuk penamaan cadangan saat Anda menggunakan konsol, layanan tidak menyalin tag dari volume, meskipun `CopyTagsToBackups` diaktifkan.

Backup dan pulihkan kinerja

Berbagai faktor dapat mempengaruhi kinerja operasi pencadangan dan pemulihan. Operasi Backup dan Restore adalah proses latar belakang, yang berarti mereka memiliki prioritas yang lebih rendah dibandingkan dengan operasi IO klien. Operasi IO klien termasuk data NFS, CIFS, dan iSCSI membaca dan menulis. Semua proses latar belakang, termasuk operasi pencadangan dan pemulihan, hanya memanfaatkan bagian yang tidak terpakai dari kapasitas throughput sistem file Anda, dan dapat memakan waktu dari beberapa menit hingga beberapa jam untuk menyelesaikannya tergantung pada ukuran cadangan Anda dan jumlah kapasitas throughput yang tidak digunakan pada sistem file Anda.

Faktor lain yang memengaruhi kinerja pencadangan dan pemulihan termasuk tingkat penyimpanan tempat data Anda disimpan dan profil kumpulan data. Kami menyarankan Anda membuat cadangan pertama volume Anda saat sebagian besar data ada di penyimpanan SSD. Dataset yang berisi sebagian besar file kecil biasanya akan memiliki kinerja yang lebih rendah dibandingkan dengan dataset berukuran sama yang sebagian besar berisi file besar. Ini karena memproses sejumlah besar file kecil menghabiskan lebih banyak siklus CPU dan overhead jaringan daripada memproses lebih sedikit file besar.

Umumnya, Anda dapat mengharapkan tingkat pencadangan berikut saat mencadangkan data yang disimpan di tingkat penyimpanan SSD:

- 750 MBps di beberapa backup bersamaan yang berisi sebagian besar file besar.
- 100 MBps di beberapa backup bersamaan yang sebagian besar berisi file kecil.

Umumnya, Anda dapat mengharapkan tingkat pemulihan berikut:

- 250 MBps di beberapa pemulihan bersamaan yang berisi sebagian besar file besar.

- 100 MBps di beberapa pemulihan bersamaan yang sebagian besar berisi file kecil.

Menggunakan AWS Backup dengan Amazon FSx

AWS Backup adalah cara sederhana dan hemat biaya untuk melindungi data Anda dengan mencadangkan Amazon FSx Anda untuk volume ONTAP. NetApp AWS Backup adalah layanan cadangan terpadu yang dirancang untuk menyederhanakan pembuatan, pemulihan, dan penghapusan cadangan, sambil memberikan pelaporan dan audit yang lebih baik. AWS Backup membuatnya lebih mudah untuk mengembangkan strategi cadangan terpusat untuk kepatuhan hukum, peraturan, dan profesional. AWS Backup juga membuat melindungi volume AWS penyimpanan, database, dan sistem file Anda lebih sederhana dengan menyediakan tempat sentral di mana Anda dapat melakukan hal berikut:

- Konfigurasikan dan audit AWS sumber daya yang ingin Anda cadangkan.
- Otomatiskan penjadwalan cadangan.
- Tetapkan kebijakan penyimpanan.
- Pantau semua aktivitas backup, penyalinan, dan pemulihan terbaru.

AWS Backup menggunakan fungsionalitas cadangan bawaan Amazon FSx. Pencadangan yang dibuat menggunakan AWS Backup konsol memiliki tingkat konsistensi dan kinerja sistem file yang sama, bersifat inkremental relatif terhadap cadangan Amazon FSx lainnya yang Anda ambil dari volume Anda (dimulai pengguna atau otomatis), dan menawarkan opsi pemulihan yang sama seperti pencadangan yang diambil melalui konsol Amazon FSx. Jika Anda menggunakannya AWS Backup untuk mengelola cadangan ini, Anda mendapatkan fungsionalitas tambahan, seperti kemampuan untuk membuat cadangan terjadwal sesering setiap jam. Anda dapat menambahkan lapisan pertahanan tambahan untuk melindungi cadangan dari penghapusan yang tidak disengaja atau berbahaya dengan menyimpannya di Vault. AWS Backup

Cadangan yang dibuat oleh dianggap sebagai cadangan AWS Backup yang diprakarsai pengguna, dan mereka dihitung terhadap kuota cadangan yang diprakarsai pengguna untuk Amazon FSx. Untuk informasi selengkapnya, lihat Kuota yang dapat Anda tingkatkan. Anda dapat melihat dan memulihkan cadangan yang dibuat oleh AWS Backup di konsol Amazon FSx, CLI, dan API. Namun, Anda tidak dapat menghapus cadangan yang dibuat oleh AWS Backup di konsol Amazon FSx, CLI, atau API. Untuk informasi selengkapnya, lihat Memulai AWS Backup di Panduan AWS Backup Pengembang.

AWS Backup tidak dapat mencadangkan volume yang offline.

Memulihkan backup ke volume baru

Anda dapat mengembalikan cadangan volume ke volume baru, secara efektif memulihkan point-in-time snapshot volume menggunakan konsol, CLI, atau API.

Saat memulihkan cadangan, semua data pertama kali ditulis ke tingkat penyimpanan SSD sebelum layanan mulai meningkatkan data ke penyimpanan kumpulan kapasitas sesuai dengan kebijakan tingkatan yang Anda tetapkan untuk volume yang dipulihkan. Saat memulihkan cadangan ke volume dengan kebijakan tieringAll, proses latar belakang periodik meningkatkan data ke kumpulan kapasitas. Saat mengembalikan cadangan ke volume dengan kebijakan tiering `Snapshot Only` atau`Auto`, data berjenjang ke kumpulan kapasitas jika pemanfaatan SSD untuk sistem file lebih besar dari 50%, dan laju pendinginan ditentukan oleh periode pendinginan kebijakan tiering.

Saat Anda mengembalikan cadangan FlexGroup volume pada sistem file yang memiliki jumlah pasangan ketersediaan tinggi (HA) yang berbeda dari sistem file asli, Amazon FSx mungkin menambahkan volume konstituen tambahan untuk memastikan bahwa konstituen didistribusikan secara merata.

Untuk step-by-step petunjuk memulihkan cadangan ke volume baru, lihatMemulihkan cadangan ke volume baru.

> **Note**
>
> Volume yang dipulihkan selalu memiliki gaya volume yang sama dengan volume aslinya. Anda tidak dapat mengubah gaya volume saat memulihkan.

Menghapus cadangan

Anda dapat menghapus backup harian otomatis dan backup volume yang diprakarsai pengguna. Menghapus cadangan adalah tindakan permanen dan tidak dapat dipulihkan. Data apapun di backup yang terhapus juga ikut dihapus. Jangan hapus cadangan kecuali Anda yakin tidak memerlukan cadangan tersebut lagi di masa mendatang. Untuk petunjuk yang menjelaskan cara menghapus cadangan, lihat. Menghapus cadangan

Anda tidak dapat menghapus cadangan yang dibuat oleh AWS Backup, yang memiliki tipe AWS Backup, di konsol Amazon FSx, CLI, atau API. Untuk informasi tentang menghapus cadangan yang dibuat oleh AWS Backup, lihat Menghapus cadangan di Panduan Pengembang. AWS Backup

Anda tidak dapat menghapus cadangan volume jika volumenya offline. Untuk informasi selengkapnya, lihat Cadangan dan volume offline.

> **Important**
>
> Jangan hapus snapshot umum pada volume karena digunakan untuk menjaga inkrementalitas di antara cadangan Anda. Menghapus snapshot umum pada volume akan menyebabkan cadangan berikutnya menjadi seluruh volume, bukan hanya cadangan tambahan.

Cadangan dan volume offline

Anda tidak dapat membuat atau menghapus cadangan volume jika volume itu offline. Gunakan perintah `volume show`ONTAPCLI untuk menentukan status dan status volume saat ini.

Untuk mengembalikan volume offline secara online, gunakan perintah `volume online`ONTAPCLI seperti pada contoh berikut:

```
::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

Membuat cadangan yang diprakarsai pengguna

Prosedur berikut menjelaskan cara menggunakan konsol Amazon FSx untuk membuat cadangan volume yang diprakarsai pengguna.

Anda tidak dapat membuat cadangan volume jika volumenya offline. Untuk informasi selengkapnya, lihat Cadangan dan volume offline.

Untuk membuat cadangan volume (konsol) yang diprakarsai pengguna

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Arahkan ke sistem File dan pilih sistem ONTAP file yang ingin Anda buat cadangan volumenya.
3. Pilih tab Volume.
4. Pilih volume yang ingin Anda cadangkan.
5. Dari Tindakan, pilih Buat backup.

6. Di kotak dialog Buat backup yang terbuka, berikan nama untuk backup Anda. Nama Backup dapat terdiri dari maksimal 256 karakter Unicode, termasuk huruf, spasi, angka, dan karakter khusus . + - = _ : /
7. Pilih Buat cadangan.

Anda sekarang telah membuat cadangan dari salah satu volume sistem file Anda. Anda dapat menemukan tabel semua cadangan Anda di konsol Amazon FSx dengan memilih Cadangan di navigasi sisi kiri. Anda dapat mencari nama yang Anda berikan pada backup Anda, dan filter tabel hanya akan menampilkan hasil yang cocok.

Ketika Anda membuat backup yang diinisiasi pengguna sebagaimana yang dijelaskan prosedur ini, backup tersebut berjenis `USER_INITIATED`, dan memiliki status `CREATING` sehingga backup menjadi sepenuhnya tersedia.

Memulihkan cadangan ke volume baru

Prosedur berikut menjelaskan cara mengembalikan fsX untuk cadangan ONTAP ke volume baru menggunakan dan. AWS Management Console AWS CLI

Untuk mengembalikan cadangan volume ke volume baru (Konsol)

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Di panel navigasi, pilih Cadangan, lalu pilih fsX untuk cadangan volume ONTAP yang ingin Anda pulihkan.
3. Di menu Tindakan kanan atas, pilih Pulihkan cadangan. Halaman Buat volume dari cadangan muncul.
4. Pilih FSx untuk sistem File ONTAP dan mesin virtual Penyimpanan yang ingin Anda pulihkan cadangan dari menu tarik-turun.
5. Di bawah Detail volume, ada beberapa pilihan. Pertama, masukkan nama Volume. Anda dapat menggunakan hingga 203 karakter alfanumerik atau garis bawah (_).
6. Untuk ukuran Volume, masukkan bilangan bulat apa pun dalam kisaran 20—314572800 untuk menentukan ukuran dalam mebibytes (MiB).
7. Untuk tipe Volume, pilih Read-Write (RW) untuk membuat volume yang dapat dibaca dan ditulis atau Perlindungan Data (DP) untuk membuat volume yang hanya-baca dan dapat digunakan sebagai tujuan hubungan atau. NetApp SnapMirror SnapVault Untuk informasi selengkapnya, lihat Tipe volume.

8. Untuk jalur Junction, masukkan lokasi di dalam sistem file untuk me-mount volume. Nama harus memiliki garis miring ke depan, misalnya`vol3`.
9. Untuk efisiensi Penyimpanan, pilih Diaktifkan untuk mengaktifkan fitur ONTAP efisiensi penyimpanan (deduplikasi, kompresi, dan pemadatan). Untuk informasi selengkapnya, lihat fsX untuk efisiensi penyimpanan ONTAP.
10. Untuk gaya keamanan Volume, pilih Unix (Linux), NTFS, atau Mixed. Gaya keamanan volume menentukan apakah preferensi diberikan ke NTFS atau UNIX ACL untuk akses multi-protokol. Mode MIXED tidak diperlukan untuk akses multi-protokol dan hanya direkomendasikan untuk pengguna tingkat lanjut.
11. Untuk kebijakan Snapshot, pilih kebijakan snapshot untuk volume. Untuk informasi selengkapnya tentang kebijakan snapshot, lihatKebijakan snapshot.

    Jika memilih Kebijakan khusus, Anda harus menentukan nama kebijakan di bidang kebijakan khusus. Kebijakan kustom harus sudah ada di SVM atau di sistem file. Anda dapat membuat kebijakan snapshot khusus dengan ONTAP CLI atau REST API. Untuk informasi selengkapnya, lihat Membuat Kebijakan Snapshot di Dokumentasi NetApp ONTAP Produk.
12. Untuk periode pendinginan kebijakan Tiering, nilai yang berlaku adalah 2-183 hari. Periode pendinginan kebijakan tingkat volume menentukan jumlah hari sebelum data yang belum diakses ditandai dingin dan dipindahkan ke penyimpanan kolam kapasitas. Pengaturan ini hanya memengaruhi `Snapshot-only` kebijakan `Auto` dan kebijakan.
13. Di bagian Lanjutan, untuk SnapLockKonfigurasi, Anda dapat meninggalkan pengaturan Nonaktif default atau memilih Diaktifkan untuk mengonfigurasi SnapLock volume. Untuk informasi selengkapnya tentang mengonfigurasi SnapLock Compliance volume atau SnapLock Enterprise volume, lihat Membuat Volume SnapLock Kepatuhan danMembuat volume SnapLock Enterprise. Untuk informasi selengkapnya tentang SnapLock, lihat Melindungi data Anda dengan SnapLock.
14. Pilih Konfirmasi untuk membuat volume.

Untuk mengembalikan cadangan volume ke volume baru (CLI)

Gunakan perintah create-volume-from-backupCLI, atau perintah CreateVolumeFromBackupAPI yang setara untuk mengembalikan cadangan volume ke volume baru.

- ```
  $ aws fsx create-volume-from-backup --backup-id backup-08e6fc1133fff3532 \
        --name demo --ontap-configuration JunctionPath=/demo, SizeInMegabytes=100000,
   \
        StorageVirtualMachineId=svm-0f04a9c7c27e1908b, TieringPolicy={Name=ALL}
  ```
  ```

Respons sistem untuk permintaan yang berhasil:


```
{
      "Volume": {
          "CreationTime": 1692721488.428,
          "FileSystemId": "fs-07ab735385276ed60",
          "Lifecycle": "CREATING",
          "Name": "demo",
          "OntapConfiguration": {
              "FlexCacheEndpointType": "NONE",
              "JunctionPath": "/demo",
              "SizeInMegabytes": 100000,
              "StorageEfficiencyEnabled": true,
              "StorageVirtualMachineId": "svm-0f04a9c7c27e1908b",
              "StorageVirtualMachineRoot": false,
              "TieringPolicy": {
                  "Name": "ALL"
              },
              "OntapVolumeType": "DP",
              "SnapshotPolicy": "default",
              "CopyTagsToBackups": false,
          },
          "ResourceARN": "arn:aws:fsx:us-east-1:752825163408:volume/
fs-07ab735385276ed60/fsvol-0b6ec764c9c5f654a",
          "VolumeId": "fsvol-0b6ec764c9c5f654a",
          "VolumeType": "ONTAP",

      }
  }
```


Menghapus cadangan

Anda dapat menghapus pencadangan harian otomatis dan pencadangan yang dimulai pengguna menggunakan konsol Amazon FSx, CLI, dan API, seperti yang dijelaskan dalam prosedur berikut.

Untuk menghapus cadangan yang dibuat menggunakan AWS Backup, lihat Menghapus cadangan di Panduan Pengembang. AWS Backup

Untuk menghapus cadangan (konsol)

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.

2. Dari dasbor konsol, pilih Backup dari navigasi sebelah kiri.
3. Pilih backup yang ingin Anda hapus dari tabel backup, dan kemudian pilih Hapus backup.
4. Di kotak dialog Hapus cadangan yang terbuka, konfirmasikan bahwa ID cadangan yang ditampilkan adalah cadangan yang ingin Anda hapus.
5. Konfirmasikan bahwa kotak centang dicentang untuk cadangan yang ingin Anda hapus.
6. Pilih Hapus backup.

Cadangan Anda dan semua data yang disertakan sekarang dihapus secara permanen dan tidak dapat dipulihkan.

Untuk menghapus cadangan (CLI)

- Gunakan perintah CLI hapus-cadangan atau tindakan DeleteBackup API yang setara untuk menghapus fsX untuk cadangan volume ONTAP, seperti yang ditunjukkan pada contoh berikut.

```
$ aws fsx delete-backup --backup-id backup-a0123456789abcdef
```

Respons sistem mencakup ID cadangan yang dihapus, dan status siklus hidupnya, dengan `DELETED` menunjukkan bahwa permintaan berhasil.

```
{
    "BackupId": "backup-a0123456789abcdef",
    "Lifecycle": "DELETED"
}
```

Cara menggunakan snapshot

Snapshot adalah gambar hanya-baca dari Amazon FSx untuk volume NetApp ONTAP pada suatu titik waktu. Snapshot menawarkan perlindungan terhadap penghapusan atau modifikasi file yang tidak disengaja dalam volume Anda. Dengan snapshot, pengguna Anda dapat dengan mudah melihat dan memulihkan file atau folder individual dari snapshot sebelumnya untuk membatalkan perubahan, memulihkan konten yang dihapus, dan membandingkan versi file.

Sebuah snapshot berisi data yang telah berubah sejak snapshot terakhir yang mengkonsumsi kapasitas penyimpanan SSD sistem file. Snapshot tidak termasuk dalam cadangan volume apa pun. Snapshot diaktifkan secara default pada volume Anda menggunakan kebijakan `default` snapshot.

Snapshot disimpan di `.snapshot` direktori di root volume. Anda dapat menyimpan maksimal 1.023 snapshot per volume kapan saja. Setelah Anda mencapai batas ini, Anda harus menghapus snapshot yang ada sebelum snapshot baru volume Anda dapat dibuat.

Topik

- Kebijakan snapshot
- Memulihkan file dan folder terpisah
- Kembalikan file dari Snapshots
- Menghapus snapshot
- Membuat kebijakan penghapusan otomatis Snapshot
- Hapus snapshot
- Menonaktifkan snapshot otomatis
- Cadangan snapshot
- Memperbarui cadangan Snapshot volume

Kebijakan snapshot

Kebijakan snapshot mendefinisikan bagaimana sistem membuat snapshot untuk volume. Kebijakan menentukan kapan harus membuat snapshot, jumlah salinan yang akan disimpan, dan cara menamainya. Ada tiga kebijakan snapshot bawaan untuk FSx untuk ONTAP:

- `default`
- `default-1weekly`
- `none`

Secara default, setiap volume dikaitkan dengan kebijakan `default` snapshot sistem file. Sebaiknya gunakan kebijakan ini untuk sebagian besar beban kerja.

`default`Kebijakan secara otomatis membuat snapshot pada jadwal berikut, dengan salinan snapshot tertua dihapus untuk memberi ruang bagi salinan yang lebih baru:

- Maksimal enam snapshot per jam diambil lima menit melewati satu jam.
- Maksimal dua foto harian diambil dari Senin hingga Sabtu pukul 10 menit setelah tengah malam.
- Maksimal dua foto mingguan diambil setiap hari Minggu pada 15 menit setelah tengah malam.

> **Note**
>
> Waktu snapshot didasarkan pada zona waktu sistem file, yang default ke Coordinated Universal Time (UTC). Untuk informasi tentang mengubah zona waktu, lihat Menampilkan dan mengatur zona waktu sistem dalam dokumentasi NetApp Support.

`default-1weekly`Kebijakan bekerja dengan cara yang sama seperti `default` kebijakan, kecuali hanya mempertahankan satu snapshot dari jadwal mingguan.

`none`Kebijakan tidak mengambil snapshot apa pun. Anda dapat menetapkan kebijakan ini ke volume untuk mencegah snapshot otomatis diambil.

Anda juga dapat membuat kebijakan snapshot khusus menggunakan ONTAP CLI atau REST API. Untuk informasi selengkapnya, lihat Membuat Kebijakan Snapshot di Dokumentasi Produk NetApp ONTAP. Anda dapat memilih kebijakan snapshot saat membuat atau memperbarui volume di konsol Amazon FSx, API, AWS CLI atau Amazon FSx. Untuk informasi selengkapnya, lihat Membuat volume dan Memperbarui volume.

Memulihkan file dan folder terpisah

Menggunakan snapshot pada sistem file Amazon FSx Anda, pengguna Anda dapat dengan cepat memulihkan versi sebelumnya dari masing-masing file atau folder. Melakukan hal ini memungkinkan mereka untuk memulihkan file yang terhapus atau diubah yang disimpan pada sistem file bersama. Mereka melakukan ini secara swalayan langsung di desktop mereka tanpa bantuan administrator. Pendekatan swalayan ini meningkatkan produktivitas dan mengurangi beban kerja administratif.

Klien Linux dan macOS dapat melihat snapshot di `.snapshot` direktori di root volume. Klien Windows dapat melihat snapshot di `Previous Versions` tab Windows Explorer (saat mengklik kanan pada file atau folder).

Kembalikan file dari Snapshots

Untuk memulihkan file dari snapshot (klien Linux dan macOS)

1. Jika file asli masih ada dan Anda tidak ingin itu ditimpa oleh file dalam snapshot, maka gunakan klien Linux atau macOS Anda untuk mengganti nama file asli atau memindahkannya ke direktori yang berbeda.
2. Di `.snapshot` direktori, cari snapshot yang berisi versi file yang ingin Anda pulihkan.

3. Salin file dari `.snapshot` direktori ke direktori di mana file awalnya ada.

Untuk mengembalikan file dari snapshot (klien Windows)

Pengguna pada klien Windows dapat memulihkan file ke versi sebelumnya menggunakan antarmuka Windows File Explorer yang sudah dikenal.

1. Untuk memulihkan file, pengguna memilih file yang akan dipulihkan, lalu pilih Pulihkan versi sebelumnya dari menu konteks (klik kanan).
2. Pengguna kemudian dapat melihat dan memulihkan ke versi sebelumnya dari daftar Versi sebelumnya.

Data dalam snapshot adalah read-only. Jika Anda ingin membuat modifikasi pada file dan folder yang tercantum di tab Versi Sebelumnya, Anda harus menyimpan salinan file dan folder yang ingin Anda modifikasi ke lokasi yang dapat ditulis dan membuat modifikasi pada salinan.

Menghapus snapshot

Snapshot mengkonsumsi kapasitas penyimpanan hanya untuk data pada volume yang telah berubah sejak snapshot terakhir. Untuk alasan ini, jika beban kerja Anda menulis data dengan cepat, snapshot dari data lama dapat mengambil sejumlah besar kapasitas penyimpanan volume.

Misalnya, output perintah `volume show-space`ONTAPCLI menunjukkan 140 KB dari. `User Data` Namun, volumenya memiliki 9, 8 GB `User Data` sebelum data pengguna dihapus. Bahkan jika Anda telah menghapus file dari volume Anda, snapshot mungkin masih mereferensikan data pengguna lama. Karena itu, `Snapshot Reserve` dan `Snapshot Spill` dalam contoh sebelumnya mengambil total 9, 8 GB ruang, meskipun hampir tidak ada data pengguna pada volume.

Untuk mengosongkan ruang pada volume, Anda dapat menghapus snapshot lama yang tidak lagi Anda perlukan. Anda dapat melakukan ini dengan membuat kebijakan penghapusan otomatis snapshot atau dengan menghapus snapshot secara manual. Menghapus snapshot menghapus data yang diubah yang disimpan pada snapshot.

Membuat kebijakan penghapusan otomatis Snapshot

Anda dapat membuat kebijakan untuk menghapus snapshot secara otomatis ketika jumlah ruang yang tersedia dalam volume Anda hampir habis. Gunakan perintah ONTAPCLI modifikasi otomatis snapshot volume untuk membuat kebijakan penghapusan otomatis untuk volume.

Saat menggunakan perintah ini, gunakan data Anda untuk mengganti nilai placeholder berikut:

- Ganti *svm_name*dengan nama SVM tempat volume dibuat.
- Ganti *vol_name*dengan nama volume.

Untuk`-trigger`, tetapkan salah satu nilai berikut:

- `volume`— Gunakan `volume` jika Anda ingin ambang batas di mana snapshot dihapus sesuai dengan total ambang kapasitas volume yang digunakan. Ambang batas kapasitas volume yang digunakan yang memicu penghapusan snapshot ditentukan oleh ukuran volume Anda, dengan penskalaan ambang batas dari 85-98 persen kapasitas yang digunakan. Volume yang lebih kecil memiliki ambang yang lebih kecil, dan volume yang lebih besar memiliki ambang yang lebih besar.
- `snap_reserve`— Gunakan `snap_reserve` jika Anda ingin snapshot dihapus berdasarkan apa yang dapat disimpan di cadangan snapshot Anda.

```
::> volume snapshot autodelete modify -vserver svm_name -volume vol_name -enabled true
 -trigger [volume|snap_reserve]
```

Untuk informasi selengkapnya, lihat perintah modifikasi hapus otomatis snapshot volume di Pusat Dokumentasi NetApp ONTAP.

Hapus snapshot

Gunakan perintah volume snapshot deleteONTAPCLI untuk menghapus snapshot secara manual, mengganti nilai placeholder berikut dengan data Anda:

- Ganti *svm_name*dengan nama SVM tempat volume dibuat.
- Ganti *vol_name*dengan nama volume.
- Ganti *snapshot_name*dengan nama snapshot. Perintah ini mendukung karakter wildcard (*) untuk *snapshot_name*. Oleh karena itu, Anda dapat menghapus semua snapshot per jam, misalnya, dengan menggunakan. `hourly*`

> **Important**
>
> Jika Anda mengaktifkan cadangan Amazon FSx, Amazon FSx mempertahankan snapshot untuk cadangan Amazon FSx terbaru dari setiap volume. Snapshot tersebut digunakan untuk

menjaga inkrementalitas di antara cadangan, dan tidak boleh dihapus dengan menggunakan metode ini.

```
FsxIdabcdef01234567892::> volume snapshot delete -vserver svm_name -volume vol_name -
snapshot snapshot_name
```

Menonaktifkan snapshot otomatis

Snapshot otomatis diaktifkan oleh kebijakan snapshot default untuk volume di fsX Anda untuk sistem file ONTAP. Jika Anda tidak memerlukan snapshot data Anda (misalnya, jika Anda menggunakan data pengujian), Anda dapat menonaktifkan snapshot dengan menyetel kebijakan snapshot volume untuk none menggunakan AWS Management Console, AWS CLI dan API, dan ONTAP CLI, seperti yang dijelaskan dalam prosedur berikut.

Untuk menonaktifkan snapshot otomatis (AWS konsol)

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Arahkan ke sistem File dan pilih sistem file ONTAP yang ingin Anda perbarui volumenya.
3. Pilih tab Volume.
4. Pilih volume yang ingin Anda perbarui.
5. Untuk Tindakan, pilih Perbarui volume.

   Kotak dialog Perbarui volume ditampilkan dengan pengaturan volume saat ini.
6. Untuk kebijakan Snapshot, pilih Tidak Ada.
7. Pilih Perbarui untuk memperbarui volume.

Untuk menonaktifkan snapshot otomatis (AWS CLI)

- Gunakan perintah AWS CLI update-volume (atau perintah API yang UpdateVolumesetara), untuk menyetel none ke, seperti `SnapshotPolicy` yang ditunjukkan pada contoh berikut.

```
aws fsx update-volume \
    --volume-id fsvol-1234567890abcdefa \
    --name new_vol \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \
           SizeInMegabytes=2048,SnapshotPolicy=none, \
```

```
            StorageEfficiencyEnabled=true, \
            TieringPolicy=all
```

Untuk menonaktifkan snapshot otomatis (ONTAPCLI)

Setel kebijakan snapshot volume untuk menggunakan kebijakan none default untuk menonaktifkan snapshot otomatis.

1. Gunakan perintah volume snapshot policy showONTAPCLI untuk menampilkan kebijakan. none

```
::> snapshot policy show -policy none

Vserver: FsxIdabcdef01234567892
                         Number of Is
Policy Name              Schedules Enabled Comment
------------------------ --------- ------- ----------------------------------
none                               0 false   Policy for no automatic snapshots.
    Schedule               Count     Prefix                 SnapMirror Label
    ---------------------- -----     ---------------------- ------------------
    -                          -     -                      -
```

2. Gunakan perintah volume modifyONTAPCLI untuk mengatur kebijakan snapshot volume none untuk menonaktifkan snapshot otomatis. Ganti nilai placeholder berikut dengan data Anda:

   - *svm_name*— gunakan nama SVM Anda.
   - *vol_name*— gunakan nama volume Anda.

   Saat diminta untuk melanjutkan, masukkan**y**.

```
::> volume modify -vserver svm_name -volume vol_name -snapshot-policy none

Warning: You are changing the Snapshot policy on volume "vol_name" to "none".
 Snapshot copies on this volume
        that do not match any of the prefixes of the new Snapshot policy will not
 be deleted. However, when
        the new Snapshot policy takes effect, depending on the new retention
 count, any existing Snapshot copies
        that continue to use the same prefixes might be deleted. See the 'volume
 modify' man page for more information.
```

```
Do you want to continue? {y|n}: y
Volume modify successful on volume vol_name of Vserver svm_name.
```

Cadangan snapshot

Cadangan salinan snapshot menetapkan persentase tertentu dari kapasitas penyimpanan volume untuk menyimpan salinan Snapshot, dengan nilai default 5 persen. Cadangan salinan Snapshot harus memiliki ruang yang cukup dialokasikan untuk salinan Snapshot, termasuk cadangan volume. Jika salinan Snapshot melebihi ruang cadangan Snapshot, Anda harus menghapus salinan Snapshot yang ada dari sistem file aktif untuk memulihkan kapasitas penyimpanan untuk penggunaan sistem file. Anda juga dapat memodifikasi persentase ruang disk yang dialokasikan ke salinan Snapshot.

Setiap kali Snapshots mengkonsumsi lebih dari 100% cadangan Snapshot, mereka mulai menempati ruang penyimpanan SSD utama. Proses ini disebut Snapshot spill. Ketika Snapshots terus menempati ruang sistem file aktif, sistem file berisiko menjadi penuh. Jika sistem file menjadi penuh karena tumpahan Snapshot, Anda dapat membuat file hanya setelah Anda menghapus cukup Snapshot.

Ketika ruang disk yang cukup tersedia untuk Snapshot dalam cadangan Snapshot, menghapus file dari tingkat SSD utama membebaskan ruang disk untuk file baru, sedangkan salinan Snapshot yang mereferensikan file-file tersebut hanya menghabiskan ruang dalam cadangan salinan Snapshot.

Karena tidak ada cara untuk mencegah Snapshot mengkonsumsi ruang disk lebih besar dari jumlah yang disediakan untuk mereka (cadangan Snapshot), penting untuk memesan ruang disk yang cukup untuk Snapshots sehingga tingkat SSD utama selalu memiliki ruang yang tersedia untuk membuat file baru atau memodifikasi yang sudah ada.

Jika Snapshot dibuat saat disk penuh, menghapus file dari tingkat SSD utama tidak menciptakan ruang kosong karena semua data itu juga direferensikan oleh Snapshot yang baru dibuat. Anda harus menghapus Snapshot untuk mengosongkan penyimpanan untuk membuat atau memperbarui file apa pun.

Anda dapat mengubah jumlah cadangan Snapshot pada volume menggunakan NetApp ONTAP CLI. Untuk informasi selengkapnya, lihat Memperbarui cadangan Snapshot volume.

Memperbarui cadangan Snapshot volume

Anda dapat mengubah jumlah cadangan Snapshot pada volume menggunakan NetApp ONTAP CLI atau API, yang dijelaskan dalam prosedur berikut.

1. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen Amazon fsX NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Untuk informasi selengkapnya, lihat Mengelola sistem file dengan ONTAP CLI.

2. Gunakan perintah `snap reserve` ONTAP CLI untuk mengubah persentase ruang disk yang digunakan untuk cadangan salinan Snapshot. Ganti *vol_name* dengan nama volume, dan *percent* `with the percent of disk space you want to reserve for Snapshot copies.`

   ```
   ::> snap reserve vol_name percent
   ```

   Contoh berikut mengubah cadangan snapshot untuk vol1 hingga 25% dari kapasitas penyimpanan volume.

   ```
   ::> snap reserve vol1 25
   ```

Replikasi terjadwal menggunakan NetApp SnapMirror

Anda dapat menggunakan NetApp SnapMirror untuk menjadwalkan replikasi berkala FSx Anda untuk sistem file ONTAP ke atau dari sistem file kedua. Kemampuan ini tersedia untuk penyebaran dalam wilayah dan lintas wilayah.

NetApp SnapMirror mereplikasi data dengan kecepatan tinggi, sehingga Anda mendapatkan ketersediaan data yang tinggi dan replikasi data yang cepat di seluruh sistem ONTAP, baik Anda mereplikasi antara dua sistem file Amazon FSx di AWS, atau dari lokal ke. AWS Replikasi dapat dijadwalkan sesering setiap 5 menit, meskipun interval harus dipilih dengan cermat berdasarkan RPO (Recovery Point Objectives), RTO (Recovery Time Objectives), dan pertimbangan kinerja.

Ketika Anda mereplikasi data ke sistem NetApp penyimpanan dan terus memperbarui data sekunder, data Anda tetap terkini dan tetap tersedia kapan pun Anda membutuhkannya. Tidak diperlukan server replikasi eksternal. Untuk informasi selengkapnya tentang penggunaan NetApp SnapMirror untuk mereplikasi data Anda, lihat Pelajari tentang layanan Replikasi dalam dokumentasi NetApp BlueXP.

Anda dapat membuat volume tujuan perlindungan data (DP) untuk NetApp SnapMirror menggunakan konsol Amazon FSx, API, AWS CLI dan Amazon FSx, selain NetApp ONTAP CLI dan REST API. Untuk informasi tentang membuat volume tujuan menggunakan konsol Amazon FSx dan AWS CLI, lihat. Membuat volume

Anda dapat menggunakan NetApp BlueXP atau NetApp ONTAP CLI untuk menjadwalkan replikasi untuk sistem file Anda.

> **Note**
>
> Ada dua jenis SnapMirror replikasi: Volume-level SnapMirror dan SVM Disaster Recovery (SVMDR). Hanya SnapMirror replikasi tingkat volume yang didukung oleh FSx untuk ONTAP.

Menggunakan NetApp BlueXP untuk menjadwalkan replikasi

Anda dapat menggunakan NetApp BlueXP untuk mengatur replikasi dengan pada fsX SnapMirror Anda untuk sistem file ONTAP. Untuk informasi selengkapnya, lihat Mereplikasi data antar sistem dalam dokumentasi NetApp BlueXP.

Menggunakan CLI NetApp ONTAP untuk menjadwalkan replikasi

Anda dapat menggunakan CLI NetApp ONTAP untuk mengonfigurasi replikasi volume terjadwal. Untuk selengkapnya, lihat Mengelola replikasi SnapMirror volume di Pusat Dokumentasi NetApp ONTAP.

Melindungi data Anda dengan SnapLock

SnapLockadalah fitur yang memungkinkan Anda untuk melindungi file Anda dengan mentransisisinya ke status tulis sekali, baca banyak (WORM), yang mencegah modifikasi atau penghapusan untuk periode retensi tertentu. Anda dapat menggunakannya SnapLock untuk memenuhi kepatuhan terhadap peraturan, untuk melindungi data penting bisnis dari serangan ransomware, dan untuk memberikan lapisan perlindungan tambahan untuk data Anda terhadap perubahan atau penghapusan.

Amazon FSx untuk NetApp ONTAP mendukung mode retensi Kepatuhan dan Perusahaan. SnapLock Lihat informasi yang lebih lengkap di Kepatuhan SnapLock dan SnapLockPerusahaan.

Anda dapat membuat SnapLock volume di FSx untuk sistem file ONTAP yang dibuat pada atau setelah 13 Juli 2023. Sistem file yang ada akan mendapatkan SnapLock dukungan selama jendela pemeliharaan mingguan mendatang.

Topik

Cara kerja SnapLock

SnapLockdapat membantu Anda memenuhi tujuan peraturan dan tata kelola dengan mencegah file Anda dihapus, diubah, atau diganti namanya. Ketika Anda membuat SnapLock volume, Anda mengkomit file Anda untuk menulis sekali, membaca banyak penyimpanan (WORM) dan mengatur periode retensi untuk data. File Anda dapat disimpan dalam keadaan yang tidak dapat dihapus, tidak dapat ditulis untuk jangka waktu yang ditentukan, atau tanpa batas waktu.

> **Important**
>
> Anda harus menentukan apakah volume akan menggunakan SnapLock pengaturan pada saat pembuatan. SnapLockNon-volume tidak dapat dikonversi ke SnapLock volume setelah pembuatan.

Mode retensi

SnapLockmemiliki dua mode retensi: Kepatuhan dan Perusahaan. Amazon FSx untuk NetApp ONTAP mendukung keduanya. Mereka memiliki kasus penggunaan yang berbeda dan beberapa fitur berbeda, tetapi keduanya melindungi data Anda dari modifikasi atau penghapusan menggunakan model WORM. Tabel berikut menjelaskan beberapa persamaan dan perbedaan antara mode retensi ini.

SnapLockfitur	Kepatuhan SnapLock	SnapLockPerusahaan
Deskripsi	File yang dialihkan ke WORM pada volume Kepatuhan tidak dapat dihapus hingga periode retensi berakhir.	File yang dialihkan ke WORM pada volume Perusahaan dapat dihapus oleh pengguna yang berwenang sebelum periode retensi mereka kedaluwarsa menggunakan penghapusan hak istimewa.
Kasus penggunaan	• Untuk mengatasi mandat khusus pemerintah atau industri seperti Aturan SEC 17a-4 (f), Aturan FINRA 4511, dan Peraturan CFTC 1.31. • Untuk melindungi dari serangan ransomware.	• Untuk memajukan integrita s data organisasi dan kepatuhan internal. • Untuk menguji setelan retensi sebelum menggunak an SnapLock Kepatuhan.
Komit otomatis	Ya	Ya
Retensi berbasis peristiwa (EBR)*	Ya	Ya
Penahanan Hukum*	Ya	Tidak
Menghapus dengan hak istimewa	Tidak	Ya
Mode Volume-append	Ya	Ya
SnapLockvolume log audit	Ya	Ya

* Operasi EBR dan Legal Hold didukung di ONTAP CLI dan REST API.

SnapLockadministrator

Anda harus memiliki hak SnapLock administrator untuk melakukan tindakan tertentu pada SnapLock volume. SnapLockhak administrator didefinisikan dalam `vsadmin-snaplock` peran dalam ONTAP CLI. Anda harus menjadi administrator cluster untuk membuat akun administrator mesin virtual penyimpanan (SVM) dengan peran SnapLock administrator.

Anda dapat melakukan tindakan berikut dengan `vsadmin-snaplock` peran dalam ONTAP CLI:

- Kelola akun pengguna, kata sandi lokal, dan informasi kunci Anda sendiri
- Kelola volume, kecuali volume bergerak
- Mengelola kuota, qtrees, salinan snapshot, dan file
- Melakukan SnapLock tindakan, termasuk penghapusan hak istimewa dan Penahanan Hukum
- Konfigurasikan protokol Network File System (NFS) dan Server Message Block (SMB)
- Konfigurasikan layanan Sistem Nama Domain (DNS), Protokol Akses Direktori Ringan (LDAP), dan Layanan Informasi Jaringan (NIS)
- Pantau pekerjaan

Prosedur berikut merinci cara membuat SnapLock administrator di ONTAP CLI. Anda harus masuk sebagai administrator klaster pada koneksi aman, seperti Secure Shell Protocol (SSH) untuk melakukan tugas ini.

Untuk membuat akun administrator SVM dengan peran vsadmin-snaplock di CLI ONTAP

- Jalankan perintah berikut. Ganti *SVM_name* dan *SnapLockAdmin*dengan informasi Anda sendiri.

```
cluster1::> security login create -vserver SVM_name -user-or-group-
name SnapLockAdmin -application ssh -authentication-method password -role vsadmin-
snaplock
```

SnapLockvolume log audit

Volume log SnapLock audit berisi log SnapLock audit, yang berisi cap waktu peristiwa seperti ketika SnapLock administrator dibuat, ketika operasi penghapusan hak istimewa dijalankan, atau ketika Penahanan Hukum ditempatkan pada file. Volume log SnapLock audit adalah catatan peristiwa yang tidak dapat dihapus.

Anda harus membuat volume log SnapLock audit dalam SVM yang sama dengan SnapLock volume untuk tindakan berikut:

- Untuk mengaktifkan atau menonaktifkan penghapusan hak istimewa pada volume SnapLock Perusahaan.
- Untuk menerapkan Penahanan Hukum pada file dalam volume SnapLock Kepatuhan.

> **Warning**
>
> - Periode retensi minimum untuk volume log SnapLock audit adalah enam bulan. Sampai periode retensi ini berakhir, volume log SnapLock audit dan SVM serta sistem file yang terkait dengannya tidak dapat dihapus meskipun volume dibuat dalam mode SnapLock Enterprise.
> - Jika file dihapus menggunakan penghapusan hak istimewa dan periode retensi lebih lama dari periode penyimpanan volume, maka volume log audit mewarisi periode penyimpanan file. Misalnya, jika file yang memiliki periode retensi 10 bulan dihapus menggunakan penghapusan hak istimewa dan periode retensi volume log audit adalah enam bulan, periode retensi volume log audit diperpanjang hingga 10 bulan.

Anda hanya dapat memiliki satu volume log SnapLock audit aktif di SVM, tetapi dapat dibagikan oleh beberapa SnapLock volume di SVM. Untuk berhasil memasang volume log SnapLock audit, atur jalur persimpangan ke`/snaplock_audit_log`. Tidak ada volume lain yang dapat menggunakan jalur persimpangan ini, termasuk volume yang bukan volume log audit.

Anda dapat menemukan log SnapLock audit di `/snaplock_log` direktori di bawah akar volume log audit. Operasi penghapusan hak istimewa dicatat di `privdel_log` subdirektori. Penahanan Hukum mulai dan operasi akhir masuk`/snaplock_log/legal_hold_logs/`. Semua log lainnya disimpan di `system_log` subdirektori.

Anda dapat membuat volume log SnapLock audit dengan konsol Amazon FSx, API Amazon fsXAWS CLI, dan CLI ONTAP dan REST API.

> **Note**
>
> Volume perlindungan data (DP) tidak dapat digunakan sebagai volume log SnapLock audit.

Prosedur berikut menjelaskan cara membuat volume log SnapLock audit di konsol Amazon FSx.

Untuk membuat volume log SnapLock audit konsol Amazon FSx

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Ikuti prosedur untuk membuat volume baru diMembuat volume.
3. Di bagian Advanced, untuk SnapLock Configuration, pilih Enabled.

   Pilih kotak centang untuk mengakui peringatan SnapLock tentang mengaktifkan volume.
4. Untuk volume log Audit, pilih Diaktifkan.

   Pastikan bahwa jalur Junction diatur ke`/snaplock_audit_log`.
5. Ikuti sisa prosedur untuk membuat volume baru diMembuat volume.
6. Pilih Konfirmasi untuk membuat volume.

Untuk mengaktifkan volume log SnapLock audit dengan Amazon FSx API, gunakan `AuditLogVolume` di file. `CreateSnaplockConfiguration`

Mengakses data Anda dalam volume SnapLock

Anda dapat menggunakan protokol file terbuka seperti NFS dan SMB untuk mengakses data Anda dalam volume. SnapLock Tidak ada dampak kinerja dari menulis data ke SnapLock volume atau dari membaca data yang dilindungi oleh WORM.

Anda dapat menyalin file di seluruh SnapLock volume dengan NFS dan SMB, tetapi mereka tidak akan mempertahankan properti WORM mereka pada volume tujuanSnapLock. Anda harus mengkomit ulang file yang disalin ke WORM untuk mencegahnya dimodifikasi atau dihapus. Untuk informasi selengkapnya, lihat Mengkomit file ke status WORM.

Anda juga dapat mereplikasi SnapLock data denganSnapMirror, tetapi volume sumber dan tujuan harus SnapLock volume dengan mode retensi yang sama (misalnya, keduanya harus Kepatuhan atau Perusahaan).

Kepatuhan SnapLock

Amazon FSx untuk NetApp ONTAP mendukung SnapLock volume Kepatuhan.

Menggunakan SnapLock Kepatuhan

Bagian ini menjelaskan kasus penggunaan dan pertimbangan untuk mode retensi Kepatuhan.

Kasus penggunaan untuk SnapLock Kepatuhan

Anda dapat memilih mode retensi Kepatuhan untuk kasus penggunaan berikut.

- Anda dapat menggunakan SnapLock Kepatuhan untuk menangani mandat khusus pemerintah atau industri seperti Aturan SEC 17a-4 (f), Aturan FINRA 4511, dan Peraturan CFTC 1.31. SnapLock Kepatuhan pada Amazon FSx untuk NetApp ONTAP dinilai untuk mandat dan peraturan ini oleh. Cohasset Associates Untuk informasi selengkapnya, lihat Laporan Penilaian Kepatuhan untuk Amazon FSx untuk NetApp ONTAP.
- Anda dapat menggunakan SnapLock Kepatuhan untuk melengkapi atau meningkatkan strategi perlindungan data yang komprehensif untuk memerangi serangan ransomware.

Pertimbangan Kepatuhan SnapLock

Berikut adalah beberapa hal penting yang perlu dipertimbangkan tentang mode retensi Kepatuhan.

- Setelah file dialihkan ke status tulis sekali, baca many (WORM) pada volume SnapLock Kepatuhan, file tersebut tidak dapat dihapus sebelum periode retensi berakhir oleh pengguna mana pun.
- Volume SnapLock Kepatuhan hanya dapat dihapus ketika periode retensi semua file WORM pada volume telah kedaluwarsa, dan file WORM telah dihapus dari volume.
- Anda tidak dapat mengganti nama volume SnapLock Kepatuhan setelah pembuatan.
- Anda dapat menggunakan SnapMirror untuk mereplikasi file WORM, tetapi volume sumber dan volume tujuan harus memiliki mode retensi yang sama (misalnya, keduanya harus Kepatuhan).
- Volume SnapLock Kepatuhan tidak dapat dikonversi ke volume SnapLock Perusahaan, dan sebaliknya.

Membuat Volume SnapLock Kepatuhan

Anda dapat membuat volume SnapLock Kepatuhan dengan konsol Amazon FSx, API Amazon fsXAWS CLI, dan CLI ONTAP dan REST API.

Untuk membuat volume SnapLock kepatuhan dengan Amazon FSx API, gunakan `SnaplockType` di file. `CreateSnaplockConfiguration`

Prosedur berikut menjelaskan cara membuat volume SnapLock Kepatuhan di konsol Amazon FSx.

Untuk membuat volume SnapLock Kepatuhan di konsol Amazon FSx

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Ikuti prosedur untuk membuat volume baru diMembuat volume.
3. Di bagian Advanced, untuk SnapLock Configuration, pilih Enabled.

   Pilih kotak centang untuk mengakui peringatan SnapLock tentang mengaktifkan volume.
4. Untuk mode Retensi, pilih Kepatuhan.
5. Untuk volume log Audit, pilih antara Diaktifkan dan Dinonaktifkan.

   Jika Anda memilih Diaktifkan, pastikan bahwa jalur Persimpangan diatur ke`/snaplock_audit_log`.

   Untuk informasi selengkapnya, lihat SnapLockvolume log audit.
6. Untuk periode Retensi, masukkan nilai untuk Retensi default, Retensi minimum, dan Retensi maksimum. Kemudian pilih Unit yang sesuai untuk masing-masing.

   Untuk informasi selengkapnya, lihat Bekerja dengan periode retensi di SnapLock.
7. Untuk Komit Otomatis, pilih antara Diaktifkan dan Dinonaktifkan.

   Jika Anda memilih Diaktifkan, untuk periode Autocommit, masukkan nilai dan pilih unit Autocommit yang sesuai.

   Anda dapat menentukan nilai antara 5 menit dan 10 tahun.

   Untuk informasi selengkapnya, lihat Komit otomatis.
8. Untuk mode Volume append, pilih antara Diaktifkan dan Dinonaktifkan.

   Untuk informasi selengkapnya, lihat Mode Volume-append.
9. Ikuti sisa prosedur untuk membuat volume baru diMembuat volume.
10. Pilih Konfirmasi untuk membuat volume.

SnapLockPerusahaan

Amazon FSx untuk NetApp ONTAP mendukung SnapLock volume Perusahaan.

Menggunakan SnapLock Enterprise

Bagian ini menjelaskan kasus penggunaan dan pertimbangan untuk mode retensi Perusahaan.

Kasus penggunaan untuk SnapLock Perusahaan

Anda dapat memilih mode retensi Perusahaan untuk kasus penggunaan berikut.

- Anda dapat menggunakan SnapLock Enterprise untuk mengotorisasi hanya pengguna tertentu untuk menghapus file.
- Anda dapat menggunakan SnapLock Enterprise untuk memajukan integritas data dan kepatuhan internal organisasi Anda.
- Anda dapat menggunakan SnapLock Enterprise untuk menguji setelan retensi sebelum menggunakan SnapLock Kepatuhan.

Pertimbangan untuk menggunakan Enterprise SnapLock

Berikut adalah beberapa hal penting yang perlu dipertimbangkan tentang mode retensi Perusahaan.

- Anda dapat menggunakan SnapMirror untuk mereplikasi file WORM, tetapi volume sumber dan volume tujuan harus memiliki mode retensi yang sama (misalnya, keduanya harus Enterprise).
- SnapLockVolume tidak dapat dikonversi dari Perusahaan ke Kepatuhan, atau dari Kepatuhan ke Perusahaan.
- SnapLockEnterprise tidak mendukung Legal Hold.

Menghapus dengan hak istimewa

Salah satu perbedaan utama antara SnapLock Perusahaan dan SnapLock Kepatuhan adalah SnapLock administrator dapat mengaktifkan penghapusan hak istimewa pada volume SnapLock Perusahaan untuk memungkinkan file dihapus sebelum periode penyimpanan file berakhir. SnapLockAdministrator adalah satu-satunya pengguna yang dapat menghapus file dari volume SnapLock Perusahaan yang memiliki kebijakan retensi aktif yang ditempatkan di dalamnya. Untuk informasi selengkapnya, lihat SnapLockadministrator.

Anda dapat mengaktifkan atau menonaktifkan penghapusan hak istimewa dengan konsol Amazon FSx, AWS CLI API Amazon FSx, dan ONTAP CLI dan REST API. Untuk mengaktifkan penghapusan hak istimewa, Anda harus terlebih dahulu membuat volume log SnapLock audit dalam SVM yang sama dengan SnapLock volume. Untuk informasi selengkapnya, lihat SnapLockvolume log audit.

Untuk mengaktifkan penghapusan hak istimewa dengan Amazon FSx API, `PrivilegedDelete` gunakan di file. `CreateSnaplockConfiguration`

Prosedur berikut menjelaskan cara mengaktifkan penghapusan hak istimewa di konsol Amazon FSx.

Untuk mengaktifkan penghapusan hak istimewa pada volume SnapLock Perusahaan di konsol Amazon FSx

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Ikuti prosedur untuk membuat volume baru diMembuat volume.
3. Di bagian Advanced, untuk SnapLock Configuration, pilih Enabled.

   Pilih kotak centang untuk mengakui peringatan SnapLock tentang mengaktifkan volume.
4. Untuk mode Retensi, pilih Enterprise.
5. Untuk Hapus Hak Istimewa, pilih Diaktifkan.
6. Ikuti sisa prosedur untuk membuat volume baru diMembuat volume.
7. Pilih Konfirmasi untuk membuat volume.

> **Note**
>
> Anda tidak dapat mengeluarkan perintah hapus dengan hak istimewa untuk menghapus file tulis sekali, baca banyak (WORM) yang memiliki periode retensi kedaluwarsa. Anda dapat mengeluarkan operasi penghapusan normal setelah periode retensi berakhir.

Anda dapat memilih untuk menonaktifkan penghapusan hak istimewa secara permanen, tetapi tindakan ini tidak dapat diubah. Jika penghapusan hak istimewa dimatikan secara permanen, Anda tidak perlu memiliki volume log SnapLock audit yang terkait dengan volume SnapLock Perusahaan.

Untuk mematikan penghapusan hak istimewa secara permanen dengan Amazon FSx API, `PrivilegedDelete` gunakan di file. `CreateSnaplockConfiguration`

Untuk mematikan penghapusan hak istimewa secara permanen pada volume SnapLock Perusahaan di konsol Amazon FSx

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.

2. Ikuti prosedur untuk membuat volume baru diMembuat volume.
3. Di bagian Advanced, untuk SnapLock Configuration, pilih Enabled.

   Pilih kotak centang untuk mengakui peringatan SnapLock tentang mengaktifkan volume.
4. Untuk mode Retensi, pilih Enterprise.
5. Untuk Hapus Hak Istimewa, pilih Dinonaktifkan secara permanen.
6. Ikuti sisa prosedur untuk membuat volume baru diMembuat volume.
7. Pilih Konfirmasi untuk membuat volume.

Membuat volume SnapLock Enterprise

Anda dapat membuat volume SnapLock Enterprise dengan konsol Amazon FSx, Amazon FSx APIAWS CLI, dan CLI ONTAP dan REST API.

Untuk membuat volume SnapLock perusahaan dengan Amazon FSx API, gunakan `SnaplockType` di file. `CreateSnaplockConfiguration`

Untuk membuat volume SnapLock Enterprise di konsol Amazon FSx

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Ikuti prosedur untuk membuat volume baru diMembuat volume.
3. Di bagian Advanced, untuk SnapLock Configuration, pilih Enabled.

   Pilih kotak centang untuk mengakui peringatan SnapLock tentang mengaktifkan volume.
4. Untuk mode Retensi, pilih Enterprise.
5. Untuk volume log Audit, pilih antara Diaktifkan dan Dinonaktifkan.

   Jika Anda memilih Diaktifkan, pastikan bahwa jalur Persimpangan diatur ke`/snaplock_audit_log`.

   Untuk informasi selengkapnya, lihat SnapLockvolume log audit.
6. Untuk periode Retensi, masukkan nilai untuk Retensi default, Retensi minimum, dan Retensi maksimum. Kemudian pilih Unit yang sesuai untuk masing-masing.

   Untuk informasi selengkapnya, lihat Bekerja dengan periode retensi di SnapLock.
7. Untuk Komit Otomatis, pilih antara Diaktifkan dan Dinonaktifkan.

Jika Anda memilih Diaktifkan, untuk periode Autocommit, masukkan nilai dan pilih unit Autocommit yang sesuai.

Anda dapat menentukan nilai antara 5 menit dan 10 tahun.

Untuk informasi selengkapnya, lihat Komit otomatis.

8. Untuk Hapus Hak Istimewa, pilih antara Diaktifkan, Dinonaktifkan, dan Dinonaktifkan secara Permanen.

   Untuk informasi selengkapnya, lihat Menghapus dengan hak istimewa.

9. Untuk mode Volume append, pilih antara Diaktifkan dan Dinonaktifkan.

   Untuk informasi selengkapnya, lihat Mode Volume-append.

10. Ikuti sisa prosedur untuk membuat volume baru diMembuat volume.
11. Pilih Konfirmasi untuk membuat volume.

Melewati mode Enterprise

Jika Anda menggunakan konsol Amazon FSx atau Amazon FSx API, Anda harus memiliki `fsx:BypassSnapLockEnterpriseRetention` izin IAM untuk menghapus volume SnapLock Perusahaan yang berisi file WORM dengan kebijakan retensi aktif.

Untuk informasi selengkapnya, lihat Menghapus volume SnapLock.

Bekerja dengan periode retensi di SnapLock

Saat membuat SnapLock volume, Anda dapat mengatur periode retensi default untuk volume, atau Anda dapat mengatur periode retensi untuk menulis sekali, membaca banyak file (WORM) secara eksplisit. Selama periode penyimpanan, Anda tidak dapat menghapus atau memodifikasi file yang dilindungi Worm. Periode retensi digunakan untuk menghitung waktu retensi. Misalnya, jika Anda mentransisikan file ke WORM pada 14 Juli 2023 pada tengah malam dan mengatur periode retensi menjadi lima tahun, maka waktu retensi akan sampai 14 Juli 2028 pada tengah malam.

Untuk informasi lebih lanjut tentang WORM, lihatMengkomit file ke status WORM.

Kebijakan periode retensi

Periode retensi ditentukan oleh nilai yang Anda tetapkan ke parameter berikut:

- Retensi default — Periode retensi default yang ditetapkan ke file WORM jika Anda tidak memberikan periode retensi eksplisit untuk file tersebut.
- Retensi minimum — Periode retensi terpendek yang dapat ditetapkan ke file WORM.
- Retensi maksimum - Periode retensi terpanjang yang dapat ditetapkan ke file WORM.

> **Note**
>
> Bahkan setelah periode retensi berakhir, Anda tidak dapat memodifikasi file WORM. Anda hanya dapat menghapusnya atau mengatur periode retensi baru untuk mengaktifkan perlindungan WORM lagi.

Anda dapat menentukan periode retensi menggunakan beberapa unit waktu yang berbeda. Tabel berikut mencantumkan rentang spesifik yang didukung.

Tipe	Nilai	Catatan
Detik	0 - 65,535	
Menit	0 - 65,535	
Jam	0 - 24	
Hari	0 - 365	
Bulan	0 -12	
Tahun	0 - 100	
Tak terbatas	-	Mempertahankan file selamanya. Tersedia untuk Retensi default, Retensi maksimum, dan Retensi minimum.

Tipe	Nilai	Catatan
Tidak ditentukan*	-	Mempertahankan file sampai Anda menetapkan periode retensi. Hanya tersedia untuk retensi default.

* Saat Anda mentransisikan file ke WORM dengan periode retensi yang tidak ditentukan, file tersebut diberikan periode retensi minimum yang dikonfigurasi untuk SnapLock volume. Saat Anda mentransisikan file yang dilindungi Worm ke waktu retensi absolut, periode retensi baru harus lebih besar dari periode minimum yang Anda tetapkan pada file sebelumnya.

Periode retensi yang kedaluwarsa

Setelah periode penyimpanan file WORM berakhir, Anda dapat menghapus file atau menetapkan periode retensi baru untuk mengaktifkan kembali perlindungan WORM. File WORM tidak dihapus secara otomatis setelah periode retensi berakhir. Anda masih tidak dapat memodifikasi konten file WORM, bahkan setelah periode retensi telah kedaluwarsa.

Mengatur periode retensi SnapLock volume

Anda dapat mengatur periode retensi SnapLock volume dengan konsol Amazon FSx, API Amazon FSxAWS CLI, dan CLI ONTAP dan REST API.

Untuk mengatur periode retensi dengan Amazon FSx API, gunakan konfigurasi. `SnaplockRetentionPeriod`

Prosedur berikut menjelaskan cara mengatur periode retensi di konsol Amazon FSx.

Untuk mengatur periode retensi SnapLock volume di konsol Amazon FSx

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Ikuti prosedur untuk membuat volume baru diMembuat volume.
3. Di bagian Advanced, untuk SnapLock Configuration, pilih Enabled.

   Pilih kotak centang untuk mengakui peringatan SnapLock tentang mengaktifkan volume.

4. Untuk periode Retensi, masukkan nilai untuk Retensi default, Retensi minimum, dan Retensi maksimum. Kemudian pilih Unit yang sesuai untuk masing-masing.
5. Ikuti sisa prosedur untuk membuat volume baru diMembuat volume.
6. Pilih Konfirmasi untuk membuat volume.

Mengkomit file ke status WORM

Bagian ini membahas bagaimana Anda dapat mentransisikan file Anda ke status tulis sekali, baca banyak (WORM). Ini juga membahas mode volume-append, yang merupakan cara untuk menulis data secara bertahap ke file yang dilindungi Worm.

Komit otomatis

Anda dapat menggunakan autocommit untuk mentransisikan file ke WORM jika file tersebut belum dimodifikasi untuk jangka waktu yang Anda tentukan. Anda dapat mengaktifkan komit otomatis dengan konsol Amazon FSx, AWS CLI API Amazon fsX, dan ONTAP CLI dan REST API.

Anda dapat menentukan periode komit otomatis antara lima menit dan 10 tahun. Tabel berikut mencantumkan rentang spesifik yang didukung.

Unit	Nilai
Menit	5 - 65,535
Jam	1 - 65,535
Hari	1 - 3,650
Bulan	1 - 120
Tahun	1 - 10

Untuk mengaktifkan komit otomatis dengan Amazon FSx API, `AutocommitPeriod` gunakan di file. `CreateSnaplockConfiguration`

Prosedur berikut menjelaskan cara mengaktifkan komit otomatis di konsol Amazon FSx.

Untuk mengaktifkan komit otomatis di konsol Amazon FSx

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Ikuti prosedur untuk membuat volume baru diMembuat volume.
3. Di bagian Advanced, untuk SnapLock Configuration, pilih Enabled.

   Pilih kotak centang untuk mengakui peringatan SnapLock tentang mengaktifkan volume.
4. Untuk Komit Otomatis, pilih Diaktifkan.
5. Untuk periode Autocommit, masukkan nilai dan pilih unit Autocommit yang sesuai.

   Anda dapat menentukan nilai antara 5 menit dan 10 tahun.
6. Ikuti sisa prosedur untuk membuat volume baru diMembuat volume.
7. Pilih Konfirmasi untuk membuat volume.

Mode Volume-append

Anda tidak dapat mengubah data yang ada dalam file yang dilindungi Worm. Namun, SnapLock memungkinkan Anda untuk mempertahankan perlindungan untuk data yang ada menggunakan file Worm-appendable. Misalnya, Anda dapat membuat file log atau menyimpan data streaming audio atau video sambil menulis data secara bertahap. Anda dapat mengaktifkan atau menonaktifkan mode volume-append dengan konsol Amazon FSx, API AWS CLI Amazon FSx, dan CLI dan REST API. ONTAP

Persyaratan untuk memperbarui mode volume-append

- SnapLockVolume harus dilepas.
- SnapLockVolume harus kosong dari salinan snapshot dan data pengguna.

Untuk mengaktifkan mode volume-append dengan Amazon FSx API, gunakan di file. `VolumeAppendModeEnabled` `CreateSnaplockConfiguration`

Prosedur berikut menjelaskan cara mengaktifkan mode volume-append di konsol Amazon FSx.

Untuk mengaktifkan mode volume-append di konsol Amazon FSx

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.

2. Ikuti prosedur untuk membuat volume baru diMembuat volume.
3. Di bagian Advanced, untuk SnapLock Configuration, pilih Enabled.

   Pilih kotak centang untuk mengakui peringatan SnapLock tentang mengaktifkan volume.
4. Untuk mode Volume append, pilih Diaktifkan.
5. Ikuti sisa prosedur untuk membuat volume baru diMembuat volume.
6. Pilih Konfirmasi untuk membuat volume.

Retensi berbasis peristiwa (EBR)

Anda dapat menggunakan retensi berbasis peristiwa (EBR) untuk membuat kebijakan khusus dengan periode retensi terkait. Misalnya, Anda dapat mentransisikan semua file di jalur tertentu ke WORM dan mengatur periode retensi selama satu tahun dengan `snaplock event-retention apply` perintah `snaplock event-retention policy create` dan. Bila Anda menggunakan EBR, Anda harus menentukan volume, direktori, atau file. Periode penyimpanan yang Anda pilih saat membuat kebijakan EBR diterapkan ke semua file di jalur yang ditentukan.

EBR didukung oleh ONTAP CLI dan REST API.

> **Note**
>
> ONTAPtidak mendukung EBR dengan FlexGroup volume.

Prosedur berikut menjelaskan cara membuat, menerapkan, memodifikasi, dan menghapus kebijakan EBR. Anda harus menjadi SnapLock administrator (memiliki `vsadmin-snaplock` peran) untuk menyelesaikan tugas-tugas ini di ONTAP CLI. Untuk informasi selengkapnya, lihat SnapLockadministrator.

Untuk membuat kebijakan EBR di CLI ONTAP

Jalankan perintah berikut. Ganti *p1* dan *“10 tahun”* dengan informasi Anda sendiri.

```
vs1::> snaplock event-retention policy create -name p1 -retention-period "10 years"
```

Untuk menerapkan kebijakan EBR di CLI ONTAP

Jalankan perintah berikut. Ganti *p1* dan *slc* dengan informasi Anda sendiri. Anda dapat menambahkan jalur setelah garis miring maju (/) jika Anda ingin menentukan jalur tertentu untuk kebijakan EBR. Jika tidak, perintah ini menerapkan kebijakan EBR ke semua file pada volume.

```
vs1::> snaplock event-retention apply -policy-name p1 -volume slc -path /
```

Untuk memodifikasi kebijakan EBR di CLI ONTAP

Jalankan perintah berikut. Ganti *p1* dan *"5 tahun"* dengan informasi Anda sendiri.

```
vs1::> snaplock event-retention policy modify -name p1 -retention-period "5 years"
```

Untuk menghapus kebijakan EBR di CLI ONTAP

Jalankan perintah berikut. Ganti *p1* dengan informasi Anda sendiri.

```
vs1::> snaplock event-retention policy delete -name p1
```

Perintah terkait di Pusat NetApp Dokumentasi:

- pembatalan retensi acara snaplock
- snaplock acara-retensi acara show-vservers
- pertunjukan retensi acara snaplock
- tampilan kebijakan retensi acara snaplock

Penahanan Hukum

Anda dapat menyimpan file WORM untuk jangka waktu yang tidak terbatas menggunakan Legal Hold. Legal Hold umumnya digunakan untuk tujuan litigasi. File WORM yang tunduk pada Penahanan Hukum tidak dapat dihapus sampai Penahanan Hukum dicabut.

Legal Hold didukung oleh ONTAP CLI dan REST API.

> **Note**
>
> ONTAPtidak mendukung Legal Hold dengan FlexGroup volume.

Prosedur berikut menjelaskan cara memulai dan mengakhiri Penahanan Hukum. Anda harus menjadi SnapLock administrator (memiliki `vsadmin-snaplock` peran) untuk menyelesaikan tugas-tugas ini di ONTAP CLI. Untuk informasi selengkapnya, lihat SnapLockadministrator.

Untuk memulai Penahanan Hukum pada file dalam volume SnapLock Kepatuhan dengan ONTAP CLI

Jalankan perintah berikut. *Ganti litigation1, slc_vol1, dan file1 dengan informasi Anda sendiri.*

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

Untuk memulai Penahanan Hukum pada semua file dalam volume SnapLock Kepatuhan dengan ONTAP CLI

Jalankan perintah berikut. Ganti *litigation1 dan slc_vol1* dengan informasi Anda sendiri.

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -path /
```

Untuk mengakhiri Penahanan Hukum pada file dalam volume SnapLock Kepatuhan dengan ONTAP CLI

Jalankan perintah berikut. *Ganti litigation1, slc_vol1, dan file1 dengan informasi Anda sendiri.*

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

Untuk mengakhiri Penahanan Hukum pada semua file dalam volume SnapLock Kepatuhan dengan ONTAP CLI

Jalankan perintah berikut. Ganti *litigation1 dan slc_vol1* dengan informasi Anda sendiri.

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -path /
```

> **Note**
>
> Kami menyarankan Anda memantau `-operation-status` dengan `snaplock legal-hold show` perintah saat mengeluarkan Penahanan Hukum untuk memastikan bahwa itu tidak gagal.

Perintah terkait di Pusat NetApp Dokumentasi:

- pembatalan penahanan hukum snaplock
- snaplock dump-file penahanan hukum
- snaplock dump-litigasi penahanan hukum
- pertunjukan penahanan hukum snaplock

Mencadangkan volume SnapLock

Anda dapat mencadangkan SnapLock volume untuk perlindungan data tambahan. Saat Anda memulihkan SnapLock volume, pengaturan asli volume — seperti retensi default, retensi minimum, dan retensi maksimum — dipertahankan. Tulis sekali, baca banyak pengaturan (WORM) dan Penahanan Hukum juga dipertahankan.

> **Note**
>
> Anda tidak dapat membuat cadangan SnapLock FlexGroup volume.

Anda dapat mengembalikan cadangan SnapLock volume sebagai SnapLock atau SnapLock non-volume. Namun, Anda tidak dapat mengembalikan cadangan SnapLock non-volume sebagai SnapLock volume.

Untuk informasi selengkapnya tentang pencadangan, lihat Menggunakan cadangan.

Menghapus volume SnapLock

Anda dapat menghapus volume SnapLock Kepatuhan jika periode retensi semua penulisan sekali, membaca banyak file (WORM) di dalamnya kedaluwarsa.

> **Note**
>
> Ketika Anda menutup Akun AWS yang berisi SnapLock Enterprise atau Compliance volume, AWS dan fsX untuk ONTAP menangguhkan akun Anda selama 90 hari dengan data Anda utuh. Jika Anda tidak membuka kembali akun selama 90 hari tersebut, AWS hapus data Anda termasuk data dalam SnapLock volume terlepas dari pengaturan retensi Anda.

Anda dapat menghapus volume SnapLock Perusahaan kapan saja jika Anda memiliki izin yang sesuai. Anda harus menjadi administrator Amazon FSx. Selain itu, apakah Anda menggunakan konsol Amazon FSx atau Amazon FSx API, Anda harus memiliki izin IAM `fsx:BypassSnapLockEnterpriseRetention` IAM untuk menghapus volume SnapLock Perusahaan yang berisi data WORM dengan kebijakan retensi aktif.

> **Warning**
>
> Periode retensi minimum untuk volume log SnapLock audit adalah enam bulan. Sampai periode retensi ini berakhir, Anda tidak dapat menghapus volume log SnapLock audit, mesin virtual penyimpanan (SVM), atau sistem file yang terkait dengan SVM—meskipun volume dibuat dalam mode Enterprise. SnapLock Untuk informasi selengkapnya, lihat SnapLockvolume log audit.

Untuk menghapus volume SnapLock Perusahaan di konsol Amazon FSx

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Di panel navigasi kiri, pilih Volume.
3. Pilih volume yang ingin Anda hapus.
4. Dari Tindakan, pilih Hapus volume.
5. Untuk Bypass Retensi SnapLock Perusahaan, pilih Ya.
6. Di kotak dialog konfirmasi, pilih salah satu opsi berikut untuk Buat cadangan akhir:
   - Pilih Ya untuk membuat cadangan akhir volume. Nama cadangan akhir ditampilkan.
   - Pilih Tidak jika Anda tidak ingin cadangan akhir volume. Anda diminta untuk mengakui bahwa setelah volume dihapus, backup otomatis tidak lagi tersedia.
7. Konfirmasikan penghapusan volume dengan memasukkan **`delete`** di bidang Konfirmasi hapus.

8. Pilih Hapus volume.

Bekerja dengan Microsoft Active Directory di FSx untuk ONTAP

Amazon FSx bekerja dengan Microsoft Active Directory untuk berintegrasi dengan lingkungan yang ada. Active Directory adalah layanan direktori Microsoft yang digunakan untuk menyimpan informasi tentang objek di jaringan, dan untuk membantu administrator dan pengguna menemukan dan menggunakan informasi ini. Objek-objek ini biasanya mencakup sumber daya bersama, seperti server file dan pengguna jaringan dan akun komputer.

Anda dapat secara opsional menggabungkan FSx Anda untuk mesin virtual penyimpanan ONTAP (SVM) ke domain Direktori Aktif Anda untuk memberikan otentikasi pengguna dan kontrol akses tingkat file dan folder. Klien blok pesan server (SMB) kemudian dapat menggunakan identitas pengguna yang ada di Active Directory untuk mengautentikasi diri mereka sendiri dan mengakses volume SVM. Pengguna Anda dapat menggunakan identitas mereka yang ada untuk mengontrol akses ke file dan folder individual. Selain itu, Anda dapat memigrasikan file dan folder yang ada serta konfigurasi daftar kontrol akses keamanan (ACL) mereka ke Amazon FSx tanpa modifikasi apa pun.

Saat Anda bergabung dengan Amazon FSx untuk NetApp ONTAP ke Direktori Aktif, Anda menggabungkan SVM sistem file ke Direktori Aktif secara independen. Ini berarti Anda dapat memiliki sistem file dengan beberapa SVM yang bergabung ke Active Directory, dan SVM lain yang tidak.

Setelah SVM bergabung ke Active Directory, Anda dapat memperbarui properti konfigurasi Active Directory berikut:

- Alamat IP server DNS
- Nama pengguna dan kata sandi akun layanan Direktori Aktif yang dikelola sendiri

Topik

Prasyarat untuk bergabung dengan SVM ke Microsoft AD yang dikelola sendiri

Sebelum Anda bergabung dengan FSx untuk ONTAP SVM ke domain Microsoft AD yang dikelola sendiri, pastikan Direktori Aktif dan jaringan Anda memenuhi persyaratan yang dijelaskan di bagian berikut.

Topik

Persyaratan Direktori Aktif lokal

Pastikan Anda sudah memiliki iklan Microsoft lokal atau yang dikelola sendiri lainnya yang dapat Anda gunakan untuk bergabung dengan SVM. Direktori Aktif ini harus memiliki konfigurasi berikut:

- Tingkat fungsional domain pengontrol domain Active Directory berada di Windows Server 2000 atau lebih tinggi.
- Active Directory menggunakan nama domain yang tidak dalam format Single Label Domain (SLD). Amazon FSx tidak mendukung domain SLD.
- Jika Anda memiliki situs Active Directory yang ditentukan, pastikan subnet di VPC yang terkait dengan fsX Anda untuk sistem file ONTAP didefinisikan di situs Active Directory yang sama, dan tidak ada konflik antara subnet VPC Anda dan subnet di situs Active Directory Anda.

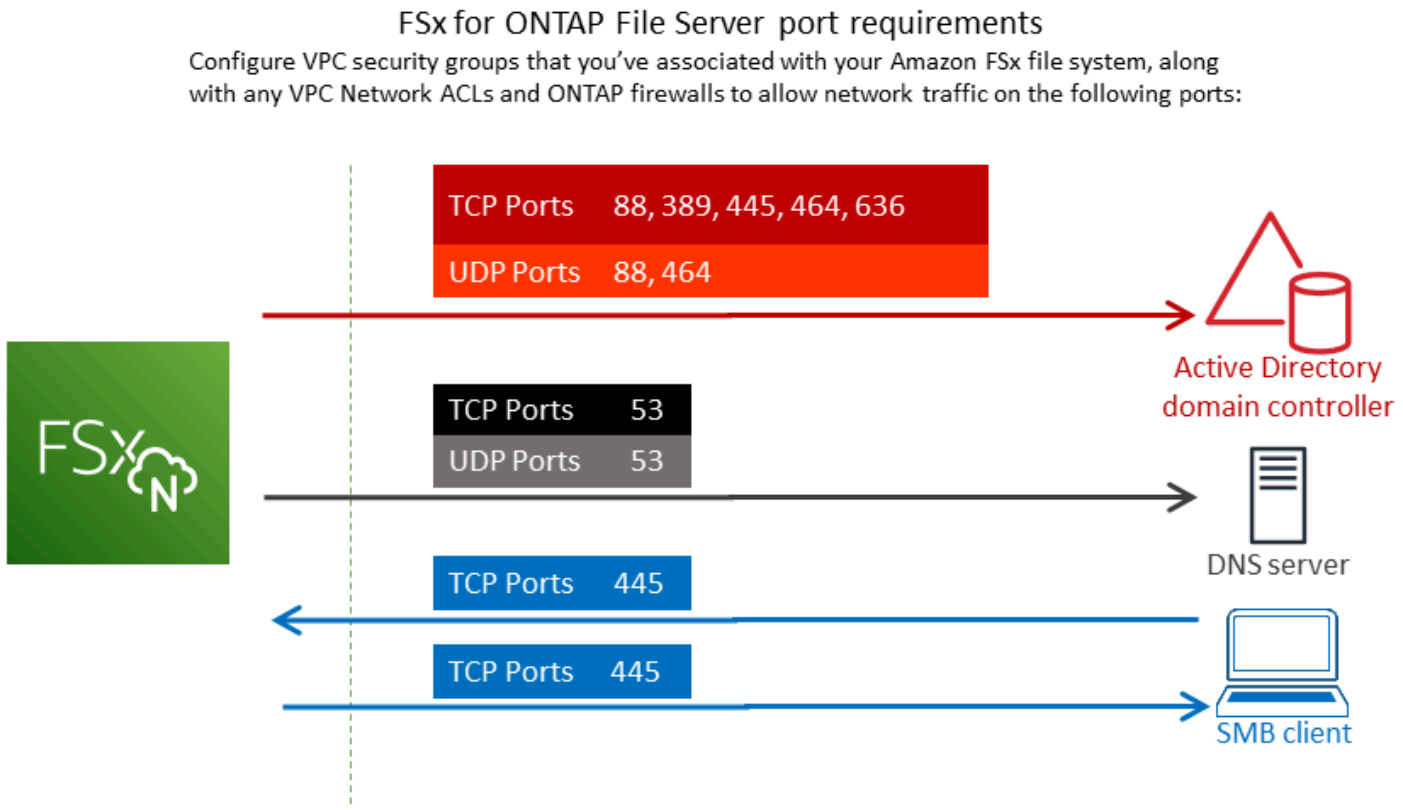
> **Note**
>
> Jika Anda menggunakan AWS Directory Service, FSx untuk ONTAP tidak mendukung penggabungan SVM ke Simple Active Directory.

Persyaratan konfigurasi jaringan

Pastikan Anda memiliki konfigurasi jaringan berikut dan informasi terkait yang tersedia untuk Anda.

> **Important**
>
> Agar SVM dapat bergabung dengan Active Directory, Anda perlu memastikan bahwa port yang didokumentasikan dalam topik ini memungkinkan lalu lintas antara semua Pengontrol Domain Direktori Aktif dan kedua alamat IP iSCSI (antarmuka logis iscsi_1 dan iscsi_2 (LIFS)) di SVM.

- Server DNS dan alamat IP pengontrol domain Direktori Aktif.
- Konektivitas antara VPC Amazon tempat Anda membuat sistem file dan Direktori Aktif yang dikelola sendiri menggunakan AWS Direct Connect,, AWS VPNatau. AWS Transit Gateway
- Grup keamanan dan ACL Jaringan VPC untuk subnet tempat Anda membuat sistem file harus mengizinkan lalu lintas pada port dan arah yang ditunjukkan pada diagram berikut.



Peran setiap port dijelaskan dalam tabel berikut.

Protokol	Port	Peran
TCP/UDP	53	Sistem Nama Domain (DNS)
TCP/UDP	88	Autentikasi Kerberos
TCP/UDP	389	Protokol Akses Direktori Ringan (LDAP)
TCP	445	Pembagian file SMB Layanan Direktori
TCP/UDP	464	Ubah/Atur kata sandi
TCP	636	Protokol Akses Direktori Ringan melalui TLS/ SSL (LDAPS)

- Aturan lalu lintas ini juga harus dicerminkan pada firewall yang berlaku untuk masing-masing pengontrol domain Active Directory, server DNS, klien FSx, dan administrator FSx.

> **Important**
>
> Sementara grup keamanan Amazon VPC memerlukan port untuk dibuka hanya dalam arah ketika lalu lintas jaringan dimulai, sebagian besar Windows firewall dan VPC ACL jaringan memerlukan port untuk terbuka di kedua arah.

Persyaratan akun layanan Direktori Aktif

Pastikan Anda memiliki akun layanan di Microsoft AD yang dikelola sendiri yang telah mendelegasikan izin untuk bergabung dengan komputer ke domain. Akun layanan adalah akun pengguna di Direktori Aktif yang dikelola sendiri yang telah didelegasikan tugas-tugas tertentu.

Minimal, akun layanan harus didelegasikan izin berikut di OU tempat Anda bergabung dengan SVM:

- Kemampuan untuk mengatur ulang kata sandi
- Kemampuan untuk membatasi akun dari membaca dan menulis data
- Kemampuan untuk mengatur `msDS-SupportedEncryptionTypes` properti pada objek komputer
- Kemampuan tervalidasi untuk menulis ke nama host DNS
- Kemampuan tervalidasi untuk menulis ke nama utama layanan

- Kemampuan untuk membuat dan menghapus objek komputer
- Kemampuan tervalidasi untuk membaca dan menulis Pembatasan Akun

Ini mewakili serangkaian izin minimum yang diperlukan untuk menggabungkan objek komputer ke Direktori Aktif Anda. Untuk informasi selengkapnya, lihat topik dokumentasi Windows Server Kesalahan: Akses ditolak ketika pengguna non-administrator yang telah didelegasikan kontrol mencoba menggabungkan komputer ke pengontrol domain.

Untuk mempelajari selengkapnya tentang membuat akun layanan dengan izin yang benar, lihat Mendelegasikan izin ke akun layanan Amazon FSx Anda.

> **Important**
>
> Amazon FSx memerlukan akun layanan yang valid di seluruh bagian sistem file Amazon FSx Anda. Amazon FSx harus dapat sepenuhnya mengelola sistem file dan melakukan tugas yang mengharuskannya untuk berhenti bergabung dan bergabung kembali dengan sumber daya ke domain Direktori Aktif Anda. Tugas-tugas ini termasuk mengganti sistem file yang gagal atau SVM, atau menambal perangkat lunak NetApp ONTAP. Perbarui informasi konfigurasi Direktori Aktif Anda dengan Amazon FSx, termasuk kredensyal akun layanan. Untuk mempelajari selengkapnya, lihat Terus memperbarui konfigurasi Direktori Aktif dengan Amazon FSx.

Jika ini adalah pertama kalinya Anda menggunakan AWS dan FSx untuk ONTAP, pastikan Anda menyelesaikan langkah penyiapan awal sebelum memulai integrasi Direktori Aktif Anda. Untuk informasi selengkapnya, lihat Menyiapkan fsX untuk ONTAP.

> **Important**
>
> Jangan pindahkan objek komputer yang dibuat Amazon FSx di OU setelah SVM Anda dibuat, atau hapus Direktori Aktif Anda saat SVM Anda bergabung dengannya. Melakukannya akan menyebabkan SVM Anda salah dikonfigurasi.

Praktik terbaik untuk bekerja dengan Active Directory

Berikut adalah beberapa saran dan pedoman yang harus Anda pertimbangkan saat bergabung dengan Amazon FSx untuk NetApp ONTAP SVM ke Microsoft Active Directory yang dikelola sendiri. Perhatikan bahwa ini direkomendasikan sebagai praktik terbaik, tetapi tidak diwajibkan.

Mendelegasikan izin ke akun layanan Amazon FSx Anda

Pastikan untuk mengonfigurasi akun layanan yang Anda berikan ke Amazon FSx dengan izin minimum yang diperlukan. Selain itu, pisahkan Unit Organisasi (OU) dari masalah pengontrol domain lainnya.

Untuk bergabung dengan Amazon FSx SVM ke domain Anda, pastikan bahwa akun layanan telah mendelegasikan izin. Anggota grup Admin Domain memiliki izin yang cukup untuk melakukan tugas ini. Namun, sebagai praktik terbaik, gunakan akun layanan yang hanya memiliki izin minimum yang diperlukan untuk melakukan ini. Prosedur berikut menunjukkan cara mendelegasikan hanya izin yang diperlukan untuk bergabung dengan FSx untuk ONTAP SVM ke domain Anda.

Lakukan prosedur ini pada mesin yang bergabung dengan direktori Anda dan menginstal snap-in Active Directory User and Computers MMC.

Untuk membuat akun layanan untuk domain Microsoft Active Directory

1. Pastikan Anda masuk sebagai administrator domain untuk domain Microsoft Active Directory Anda.
2. Buka MMC snap-in Pengguna Direktori Aktif dan Komputer.
3. Dalam panel tugas, perluas simpul domain.
4. Temukan dan buka menu konteks (klik kanan) untuk OU yang ingin Anda ubah, lalu pilih Delegasikan Kontrol.
5. Pada halaman Delegasi Control Wizard, pilih Selanjutnya.
6. Pilih Tambahkan untuk menambahkan pengguna tertentu atau grup tertentu untuk Pengguna dan grup yang dipilih, lalu pilih Selanjutnya.
7. Pada halaman Tugas untuk Didelegasikan, pilih Buat tugas kustom untuk didelegasikan, lalu pilih Selanjutnya.
8. Pilih Hanya objek berikut dalam folder, lalu pilih Objek komputer.
9. Pilih Buat objek yang dipilih dalam folder ini dan Hapus objek yang dipilih dalam folder ini. Lalu pilih Berikutnya.

10. Di bawah Tampilkan izin ini, pastikan bahwa Umum dan Properti spesifik dipilih.
11. Untuk Izin, pilih:

    - Setel Ulang Kata Sandi
    - Baca dan tulis Pembatasan Akun
    - Menulis tervalidasi ke nama host DNS
    - Menulis tervalidasi ke nama utama layanan
    - Tulis MSDs- SupportedEncryptionTypes
12. Pilih Selanjutnya, dan kemudian pilih Selesai.
13. Tutup snap-in Active Directory User and Computers MMC.

> **Important**
>
> Jangan pindahkan objek komputer yang dibuat Amazon FSx di OU setelah SVM Anda dibuat. Melakukannya akan menyebabkan SVM Anda salah dikonfigurasi.

Terus memperbarui konfigurasi Direktori Aktif dengan Amazon FSx

Untuk ketersediaan SVM Amazon FSx tanpa gangguan, perbarui konfigurasi Active Directory (AD) SVM yang dikelola sendiri saat Anda mengubah pengaturan AD yang dikelola sendiri.

Misalnya, ketika AD Anda menggunakan kebijakan pengaturan ulang kata sandi berbasis waktu. Dalam kasus ini, segera setelah kata sandi diatur ulang, pastikan untuk memperbarui kata sandi akun layanan dengan Amazon FSx. Untuk melakukannya, gunakan konsol Amazon FSx, Amazon FSx API, atau AWS CLI. Demikian pula, jika alamat IP server DNS berubah untuk domain Direktori Aktif Anda, segera setelah perubahan terjadi perbarui alamat IP server DNS dengan Amazon FSx.

Jika ada masalah dengan konfigurasi AD yang dikelola sendiri yang diperbarui, status SVM akan beralih ke Salah Konfigurasi. Status ini menampilkan pesan kesalahan dan tindakan yang disarankan di samping deskripsi SVM di konsol, API, dan CLI. Jika terjadi masalah dengan konfigurasi AD SVM Anda, pastikan untuk mengambil tindakan korektif yang disarankan untuk properti konfigurasi. Jika masalah teratasi, verifikasi bahwa status SVM Anda berubah menjadi Dibuat.

Untuk informasi selengkapnya, silakan lihat Memperbarui konfigurasi SVM Active Directory yang ada menggunakan AWS Management Console, AWS CLI, dan API dan Memodifikasi konfigurasi Active Directory menggunakan ONTAP CLI.

Menggunakan grup keamanan untuk membatasi lalu lintas dalam VPC

Untuk membatasi lalu lintas jaringan di virtual private cloud (VPC) Anda, Anda dapat menerapkan prinsip pengurangan hak istimewa dalam VPC Anda. Dengan kata lain, Anda dapat membatasi izin ke yang minimum yang diperlukan. Untuk melakukannya, gunakan aturan grup keamanan. Untuk mempelajari selengkapnya, lihat Grup keamanan Amazon VPC.

Membuat aturan grup keamanan keluar untuk antarmuka jaringan sistem file Anda

Untuk keamanan yang lebih besar, pertimbangkan untuk mengkonfigurasi grup keamanan dengan aturan lalu lintas keluar. Aturan ini harus mengizinkan lalu lintas keluar hanya ke pengontrol domain AD yang dikelola sendiri atau dalam subnet atau grup keamanan. Terapkan grup keamanan ini ke VPC yang terkait dengan antarmuka jaringan elastis sistem file Amazon FSx Anda. Untuk mempelajari informasi lebih lanjut, lihat Kontrol Akses Sistem File dengan Amazon VPC.

Bergabung dengan SVM ke Microsoft Active Directory

Organisasi Anda mungkin mengelola identitas dan perangkat menggunakan Active Directory, baik lokal maupun di cloud. Dengan FSx untuk ONTAP, Anda dapat bergabung dengan SVM Anda langsung ke domain Active Directory yang ada dengan cara berikut:

- Bergabung dengan SVM baru ke Active Directory saat pembuatan:
  - Menggunakan opsi Buat Standar di konsol Amazon FSx untuk membuat fsX baru untuk sistem file ONTAP, Anda dapat menggabungkan SVM default ke Direktori Aktif yang dikelola sendiri. Untuk informasi selengkapnya, lihat Untuk membuat sistem file (konsol).
  - Menggunakan konsol Amazon FSx, AWS CLI, atau Amazon FSx API untuk membuat SVM baru pada sistem file FSx untuk ONTAP yang ada. Untuk informasi selengkapnya, lihat Membuat mesin virtual penyimpanan.
- Bergabung dengan SVM yang ada ke Active Directory:
  - Menggunakan AWS Management Console, AWS CLI, dan API untuk menggabungkan SVM ke Direktori Aktif, dan mencoba kembali menggabungkan SVM ke Direktori Aktif jika upaya awal untuk bergabung gagal. Anda juga dapat memperbarui beberapa properti konfigurasi Active Directory untuk SVM yang sudah bergabung ke Active Directory. Untuk informasi selengkapnya, lihat Mengelola konfigurasi SVM Active Directory.

- Menggunakan NetApp ONTAP CLI atau REST API untuk bergabung, mencoba kembali bergabung, dan memutuskan konfigurasi SVM Active Directory. Untuk informasi selengkapnya, lihat Mengelola konfigurasi SVM Active Directory Anda menggunakan CLI NetApp .

> **Important**
>
> - Amazon FSx hanya mendaftarkan catatan DNS untuk SVM jika Anda menggunakan Microsoft DNS sebagai layanan DNS default. Jika Anda menggunakan DNS pihak ketiga, Anda harus menyiapkan entri DNS secara manual untuk Amazon FSx SVM setelah Anda membuatnya.
> - Jika Anda menggunakan AWS Managed Microsoft AD, Anda harus menentukan grup seperti Administrator FSx AWS Delegasi, Administrator Delegasi AWS , atau grup kustom dengan izin yang didelegasikan ke OU.

Saat Anda bergabung dengan FSx untuk ONTAP SVM langsung ke Direktori Aktif yang dikelola sendiri, SVM berada di hutan Direktori Aktif yang sama (wadah paling logis teratas dalam konfigurasi Direktori Aktif yang berisi domain, pengguna, dan komputer) dan dalam domain Direktori Aktif yang sama dengan pengguna dan sumber daya yang ada, termasuk server file yang ada.

Informasi yang dibutuhkan saat bergabung dengan SVM ke Active Directory

Anda harus memberikan informasi berikut tentang Active Directory saat menggabungkan SVM ke Active Directory, terlepas dari operasi API yang Anda pilih:

- Nama NetBIOS dari objek komputer Active Directory yang akan dibuat untuk SVM Anda. Ini adalah nama SVM di Active Directory, yang harus unik dalam Active Directory Anda. Jangan gunakan nama NetBIOS dari domain rumah. Nama NetBIOS tidak boleh melebihi 15 karakter.
- Nama domain yang sepenuhnya memenuhi syarat (FQDN) dari Direktori Aktif Anda. FQDN tidak dapat melebihi 255 karakter.

  > **Note**
  >
  > FQDN tidak dapat dalam format Single Label Domain (SLD). Amazon FSx tidak mendukung domain SLD.

- Hingga tiga alamat IP server DNS atau host domain untuk domain Anda.

Alamat IP server DNS dan alamat IP pengontrol domain Direktori Aktif dapat berada dalam rentang alamat IP apa pun, kecuali:

- Alamat IP yang bertentangan dengan alamat IP milik Amazon Web Services di dalamnya. Wilayah AWS Untuk daftar alamat AWS IP menurut Wilayah, lihat rentang alamat AWS IP.
- Alamat IP dalam rentang blok CIDR berikut: 198.19.0.0/16

- Nama pengguna dan kata sandi untuk akun layanan di domain Direktori Aktif Anda untuk Amazon FSx untuk digunakan saat bergabung dengan SVM ke domain Direktori Aktif. Untuk informasi selengkapnya tentang persyaratan akun layanan, lihatPersyaratan akun layanan Direktori Aktif.
- (Opsional) Unit Organisasi (OU) di domain tempat Anda bergabung dengan SVM.

> **Note**
>
> Jika Anda menggabungkan SVM Anda ke AWS Directory Service Active Directory, Anda harus memberikan OU yang berada dalam OU default yang AWS Directory Service membuat objek direktori yang terkait AWS dengan. Ini karena AWS Directory Service tidak menyediakan akses ke `Computers` OU default Active Directory Anda. Misalnya, jika domain Active Directory Anda`example.com`, Anda dapat menentukan OU berikut:`OU=Computers,OU=example,DC=example,DC=com`.

- (Opsional) Grup domain tempat Anda mendelegasikan wewenang untuk melakukan tindakan administratif pada sistem file Anda. Misalnya, grup domain ini mungkin mengelola berbagi file SMB Windows, mengambil kepemilikan file dan folder, dan sebagainya. Jika Anda tidak menentukan grup ini, Amazon FSx mendelegasikan otoritas ini ke grup Admin Domain di domain Direktori Aktif Anda secara default.

Mengelola konfigurasi SVM Active Directory

Bagian ini menjelaskan cara menggunakan AWS Management Console,, FSx API AWS CLI, dan CLI ONTAP untuk melakukan hal berikut:

- Bergabung dengan SVM yang sudah ada ke Active Directory
- Memodifikasi konfigurasi SVM Active Directory yang ada
- Menghapus SVM dari Active Directory

Untuk menghapus SVM dari Active Directory, Anda harus menggunakan NetApp ONTAP CLI.

Topik

Bergabung dengan SVM ke Active Directory menggunakan AWS Management Console, AWS CLI dan API

Gunakan prosedur berikut untuk menggabungkan SVM yang ada ke Active Directory. Dalam prosedur ini, SVM belum bergabung dengan Active Directory.

Untuk bergabung dengan SVM ke Active Directory () AWS Management Console

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Pilih SVM yang ingin Anda gabungkan ke Active Directory:
   - Di panel navigasi kiri, pilih Sistem file, lalu pilih sistem file ONTAP dengan SVM yang ingin Anda perbarui.
   - Pilih tab Storage Virtual Machines.

   —Atau—

   - Untuk menampilkan daftar semua SVM yang tersedia, di panel navigasi kiri, perluas ONTAP dan pilih mesin virtual Penyimpanan. Daftar semua SVM di akun Anda di Wilayah AWS ditampilkan.

   Pilih SVM yang ingin Anda gabungkan ke Active Directory dari daftar.
3. Di kanan atas panel Ringkasan SVM, pilih Tindakan > Gabung/Perbarui Direktori Aktif. Jendela Join SVM ke Active Directory muncul.
4. Masukkan informasi berikut untuk Active Directory tempat Anda bergabung dengan SVM:
   - Nama NetBIOS dari objek komputer Active Directory yang akan dibuat untuk SVM Anda. Ini adalah nama SVM di Active Directory, yang harus unik dalam Active Directory Anda. Jangan gunakan nama NetBIOS dari domain rumah. Nama NetBIOS tidak boleh melebihi 15 karakter.

- Nama domain yang sepenuhnya memenuhi syarat (FQDN) dari Direktori Aktif Anda. Nama domain tidak boleh melebihi 255 karakter.
- Alamat IP server DNS — Alamat IPv4 dari server DNS untuk domain Anda.
- Nama pengguna akun layanan — Nama pengguna akun layanan di Direktori Aktif Anda yang ada. Jangan sertakan awalan atau akhiran domain. Misalnya, untuk`EXAMPLE\ADMIN`, gunakan saja`ADMIN`.
- Kata sandi akun layanan — Kata sandi untuk akun layanan.
- Konfirmasi kata sandi — Kata sandi untuk akun layanan.
- (Opsional) Unit Organisasi (OU) - Nama jalur terhormat dari unit organisasi tempat Anda ingin bergabung dengan SVM Anda.
- Grup administrator sistem file yang didelegasikan — Nama grup di Direktori Aktif Anda yang dapat mengelola sistem file Anda.

  Jika Anda menggunakan AWS Managed Microsoft AD, Anda harus menentukan grup seperti Administrator FSx AWS Delegasi, Administrator Delegasi AWS , atau grup kustom dengan izin yang didelegasikan ke OU.

  Jika Anda bergabung ke Active Directory yang dikelola sendiri, gunakan nama grup di Active Directory Anda. Grup defaultnya adalah`Domain Admins`.

5. Pilih Gabung Active Directory untuk bergabung dengan SVM ke Active Directory menggunakan konfigurasi yang Anda berikan.

Untuk bergabung dengan SVM ke Active Directory (AWS CLI)

- Untuk menggabungkan FSx untuk ONTAP SVM ke Active Directory, gunakan perintah update-storage-virtual-machineCLI (atau operasi UpdateStorageVirtualMachineAPI yang setara), seperti yang ditunjukkan pada contoh berikut.

```
aws fsx update-storage-virtual-machine \
  --storage-virtual-machine-id svm-abcdef0123456789a\
  --active-directory-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
    OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",
\
    FileSystemAdministratorsGroup="FSxAdmins",UserName="FSxService",\
    Password="password", \
    DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

Setelah berhasil membuat mesin virtual penyimpanan, Amazon FSx mengembalikan deskripsinya dalam format JSON, seperti yang ditunjukkan pada contoh berikut.


```
{
  "StorageVirtualMachine": {
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
```

```
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATED",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef0123456789a",
    "StorageVirtualMachineId": "svm-abcdef0123456789a",
    "Subtype": "default",
    "Tags": [],

  }
}
```

Memperbarui konfigurasi SVM Active Directory yang ada menggunakan AWS Management Console, AWS CLI, dan API

Gunakan prosedur berikut untuk memperbarui konfigurasi Active Directory dari SVM yang sudah bergabung ke Active Directory.

Untuk memperbarui konfigurasi SVM Active Directory () AWS Management Console

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Pilih SVM yang akan diperbarui sebagai berikut:

   - Di panel navigasi kiri, pilih Sistem file, lalu pilih sistem file ONTAP dengan SVM yang ingin Anda perbarui.
   - Pilih tab Storage Virtual Machines.

   —Atau—

   - Untuk menampilkan daftar semua SVM yang tersedia, di panel navigasi kiri, perluas ONTAP dan pilih mesin virtual Penyimpanan.

   Pilih SVM yang ingin Anda perbarui dari daftar.
3. Pada panel Ringkasan SVM, pilih Tindakan > Gabung/Perbarui Direktori Aktif. Jendela konfigurasi Update SVM Active Directory muncul.
4. Anda dapat memperbarui properti konfigurasi Active Directory berikut di jendela ini.

   - Alamat IP server DNS — Alamat IPv4 dari server DNS untuk domain Anda.

- Nama pengguna akun layanan — Nama pengguna akun layanan di Direktori Aktif Anda yang ada. Jangan sertakan awalan atau akhiran domain. Untuk`EXAMPLE\ADMIN`, gunakan`ADMIN`.
- Kata sandi akun layanan — Kata sandi untuk akun layanan Active Directory.

5. Setelah Anda memasukkan pembaruan, pilih Perbarui Direktori Aktif untuk membuat perubahan.

Gunakan prosedur berikut untuk memperbarui konfigurasi Active Directory dari SVM yang sudah bergabung ke Active Directory.

Untuk memperbarui konfigurasi SVM Active Directory () AWS CLI

- Untuk memperbarui konfigurasi Direktori Aktif SVM dengan AWS CLI atau API, gunakan perintah update-storage-virtual-machineCLI (atau operasi API yang UpdateStorageVirtualMachinesetara), seperti yang ditunjukkan pada contoh berikut.

```
aws fsx update-storage-virtual-machine \
    --storage-virtual-machine-id svm-abcdef0123456789a\
    --active-directory-configuration \
    SelfManagedActiveDirectoryConfiguration='{UserName="FSxService",\
    Password="password", \
    DnsIps=["10.0.1.18"]}'
```

Mengelola konfigurasi SVM Active Directory Anda menggunakan CLI NetApp

Anda dapat menggunakan CLI NetApp ONTAP untuk bergabung dan memutuskan sambungan SVM Anda ke Active Directory, dan untuk memodifikasi konfigurasi SVM Active Directory yang ada.

Bergabung dengan SVM ke Active Directory menggunakan ONTAP CLI

Anda dapat menggabungkan SVM yang ada ke Direktori Aktif menggunakan CLI ONTAP, seperti yang dijelaskan dalam prosedur berikut. Anda dapat melakukan ini bahkan jika SVM Anda sudah bergabung ke Active Directory.

1. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen Amazon fsX NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *`management_endpoint_ip`* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat Mengelola sistem file dengan ONTAP CLI.

2. Buat entri DNS untuk Active Directory Anda dengan memberikan nama DNS direktori lengkap (`corp.example.com`) dan setidaknya satu alamat IP server DNS.

```
::>vserver services name-service dns create -vserver svm_name -
domains corp.example.com -name-servers dns_ip_1, dns_ip_2
```

Untuk memverifikasi koneksi ke server DNS Anda, jalankan perintah berikut. Ganti *svm_name dengan informasi* Anda sendiri.

```
FsxId0ae30e5b7f1a50b6a::>vserver services name-service dns check -vserver svm_name

                            Name Server
Vserver       Name Server     Status       Status Details
------------- --------------- ------------ --------------------------
svm_name      172.31.14.245   up           Response time (msec): 0
svm_name      172.31.25.207   up           Response time (msec): 1
2 entries were displayed.
```

3. Untuk menggabungkan SVM Anda ke Active Directory, jalankan perintah berikut. Perhatikan bahwa Anda harus menentukan `computer_name` yang belum ada di Active Directory Anda dan memberikan nama DNS direktori untuk`-domain`. Untuk`-OU`, masukkan OU yang Anda inginkan untuk bergabung dengan SVM, serta nama DNS lengkap dalam format DC.

```
::>vserver cifs create -vserver svm_name -cifs-server computer_name -
domain corp.example.com -OU OU=Computers,OU=example,DC=corp,DC=example,DC=com
```

Untuk memverifikasi status koneksi Active Directory Anda, jalankan perintah berikut:

```
::>vserver cifs check -vserver svm_name

              Vserver : svm_name
            Cifs NetBIOS Name : svm_netBIOS_name
                  Cifs Status : Running
                         Site : Default-First-Site-Name
Node Name       DC Server Name  DC Server IP    Status   Status Details
--------------- --------------  --------------- ------   --------------
```

```
FsxId0ae30e5b7f1a50b6a-01
                corp.example.com
                                172.31.14.245   up       Response time (msec): 5
FsxId0ae30e5b7f1a50b6a-02
                corp.example.com
                                172.31.14.245   up       Response time (msec): 20
2 entries were displayed.
```

4. Jika Anda tidak dapat mengakses berbagi setelah bergabung ini, tentukan apakah akun yang Anda gunakan untuk mengakses berbagi memiliki izin. Misalnya, jika Anda menggunakan `Admin` akun default (administrator yang didelegasikan) dengan Direktori Aktif AWS terkelola, Anda harus menjalankan perintah berikut di ONTAP. `netbios_domain`Sesuai dengan nama domain Active Directory Anda (untuk`corp.example.com`, yang `netbios_domain` digunakan di sini adalah`example`).

```
FsxId0123456789a::>vserver cifs users-and-groups local-group add-members -vserver
 svm_name -group-name BUILTIN\Administrators -member-names netbios_domain\admin
```

Memodifikasi konfigurasi Active Directory menggunakan ONTAP CLI

Anda dapat menggunakan CLI ONTAP untuk memodifikasi konfigurasi Active Directory yang ada.

1. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen Amazon fsX NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *`management_endpoint_ip`* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

   Untuk informasi selengkapnya, lihat Mengelola sistem file dengan ONTAP CLI.

2. Jalankan perintah berikut untuk menurunkan server CIFS SVM sementara:

```
FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
```

3. Jika Anda perlu memodifikasi entri DNS Active Directory Anda, jalankan perintah berikut:

```
::>vserver services name-service dns modify -vserver svm_name -
domains corp.example.com -name-servers dns_ip_1,dns_ip_2
```

Anda dapat memvalidasi status koneksi ke server DNS Active Directory menggunakan perintah. `vserver services name-service dns check -vserver svm_name`

```
::>vserver services name-service dns check -vserver svm_name
                              Name Server
Vserver       Name Server     Status       Status Details
------------- --------------- ------------ --------------------------
svmciad       dns_ip_1        up           Response time (msec): 1
svmciad       dns_ip_2        up           Response time (msec): 1
2 entries were displayed.
```

4. Jika Anda perlu memodifikasi konfigurasi Active Directory itu sendiri, Anda dapat mengubah bidang yang ada dengan menggunakan perintah berikut, menggantikan:

   - *computer_name*, jika Anda ingin memodifikasi nama NetBIOS (akun mesin) SVM.
   - *domain_name*, jika Anda ingin memodifikasi nama domain. Ini harus sesuai dengan entri domain DNS yang dicatat dalam Langkah 3 bagian ini (`corp.example.com`).
   - `organizational_unit`, jika Anda ingin memodifikasi OU (`OU=Computers,OU=example,DC=corp,DC=example,DC=com`).

   Anda harus memasukkan kembali kredensyal Active Directory yang Anda gunakan untuk bergabung dengan perangkat ini ke Active Directory.

   ```
   ::>vserver cifs modify -vserver svm_name -cifs-server computer_name -
   domain domain_name -OU organizational_unit
   ```

   Anda dapat memverifikasi status koneksi koneksi Direktori Aktif Anda menggunakan `vserver cifs check -vserver svm_name` perintah.

5. Ketika Anda selesai memodifikasi Active Directory dan konfigurasi DNS Anda, bawalah server CIFS kembali dengan menjalankan perintah berikut:

   ```
   ::>vserver cifs modify -vserver svm_name -status-admin up
   ```

Berhenti bergabung dengan Active Directory dari SVM Anda menggunakan ONTAP NetApp CLI

CLI NetApp ONTAP juga dapat digunakan untuk memutuskan sambungan SVM Anda dari Active Directory dengan mengikuti langkah-langkah di bawah ini:

1. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen Amazon fsX NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Untuk informasi selengkapnya, lihat Mengelola sistem file dengan ONTAP CLI.

2. Hapus server CIFS yang melepaskan perangkat Anda dari Active Directory dengan menjalankan perintah berikut. Agar ONTAP menghapus akun mesin untuk SVM Anda, berikan kredensyal yang awalnya Anda gunakan untuk bergabung dengan SVM ke Direktori Aktif.

   ```
   FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
   ```

3. Jika Anda perlu memodifikasi entri DNS Active Directory Anda, jalankan perintah berikut:

   ```
   FsxId0123456789a::vserver cifs delete -vserver svm_name

   In order to delete an Active Directory machine account for the CIFS server, you
    must supply the name and password of a Windows account with
   sufficient privileges to remove computers from the "CORP.ADEXAMPLE.COM" domain.

   Enter the user name: user_name

   Enter the password:

   Warning: There are one or more shares associated with this CIFS server
            Do you really want to delete this CIFS server and all its shares? {y|n}: y
   ```

4. Hapus server DNS untuk Active Directory Anda dengan menjalankan perintah berikut:

   ```
   ::vserver services name-service dns delete -vserver svm_name
   ```

Jika Anda melihat peringatan seperti berikut—yang menunjukkan bahwa `dns` harus dihapus sebagai `ns-switch` —dan Anda tidak berencana untuk bergabung kembali dengan perangkat ini ke Direktori Aktif, Anda dapat menghapus entri. `ns-switch`

```
Warning: "DNS" is present as one of the sources in one or more ns-switch databases
 but no valid DNS configuration was found for Vserver
         "svm_name". Remove "DNS" from ns-switch using the "vserver services name-
service ns-switch" command. Configuring "DNS" as a source
         in the ns-switch setting when there is no valid configuration can cause
 protocol access issues.
```

5. (Opsional) Hapus `ns-switch` entri `dns` dengan menjalankan perintah berikut. Verifikasi urutan sumber, lalu hapus `dns` entri untuk `hosts` database dengan memodifikasi `sources` sehingga hanya berisi sumber lain yang terdaftar. Dalam contoh ini, satu-satunya sumber lainnya adalah`files`.

```
::>vserver services name-service ns-switch show -vserver svm_name -database hosts

                    Vserver: svm_name
Name Service Switch Database: hosts
   Name Service Source Order: files, dns
```

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts
 -sources files
```

6. (Opsional) Hapus `dns` entri dengan memodifikasi host database untuk disertakan saja`files`. `sources`

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts
 -sources files
```

Amazon FSx untuk NetApp kinerja ONTAP

Berikut ini adalah ikhtisar Amazon FSx untuk kinerja sistem file NetApp ONTAP, dengan diskusi tentang opsi kinerja dan throughput yang tersedia serta tip kinerja yang berguna.

Topik

Bagaimana kinerja diukur untuk FSx untuk sistem file ONTAP

Performa sistem file diukur dengan latensi, throughput, dan operasi I/O per detik (IOPS).

Latensi

Amazon FSx untuk NetApp ONTAP menyediakan latensi operasi file sub-milidetik dengan penyimpanan solid state drive (SSD), dan latensi puluhan milidetik untuk penyimpanan kolam kapasitas. Di atas itu, Amazon FSx memiliki dua lapisan cache baca pada setiap server file — drive NVMe (non-volatile memory express) dan in-memory — untuk memberikan latensi yang lebih rendah saat Anda mengakses data yang paling sering dibaca.

Throughput dan IOPS

Setiap sistem file Amazon FSx menyediakan hingga puluhan GB/s throughput dan jutaan IOPS. Jumlah spesifik throughput dan IOPS yang dapat dikendarai oleh beban kerja Anda pada sistem file Anda tergantung pada total kapasitas throughput dan konfigurasi kapasitas penyimpanan sistem file Anda, bersama dengan sifat beban kerja Anda, termasuk ukuran set kerja aktif.

SMB Multichannel dan dukungan NFS nconnect

Dengan Amazon FSx, Anda dapat mengonfigurasi SMB Multichannel untuk menyediakan beberapa koneksi antara ONTAP dan klien dalam satu sesi SMB. SMB Multichannel menggunakan beberapa

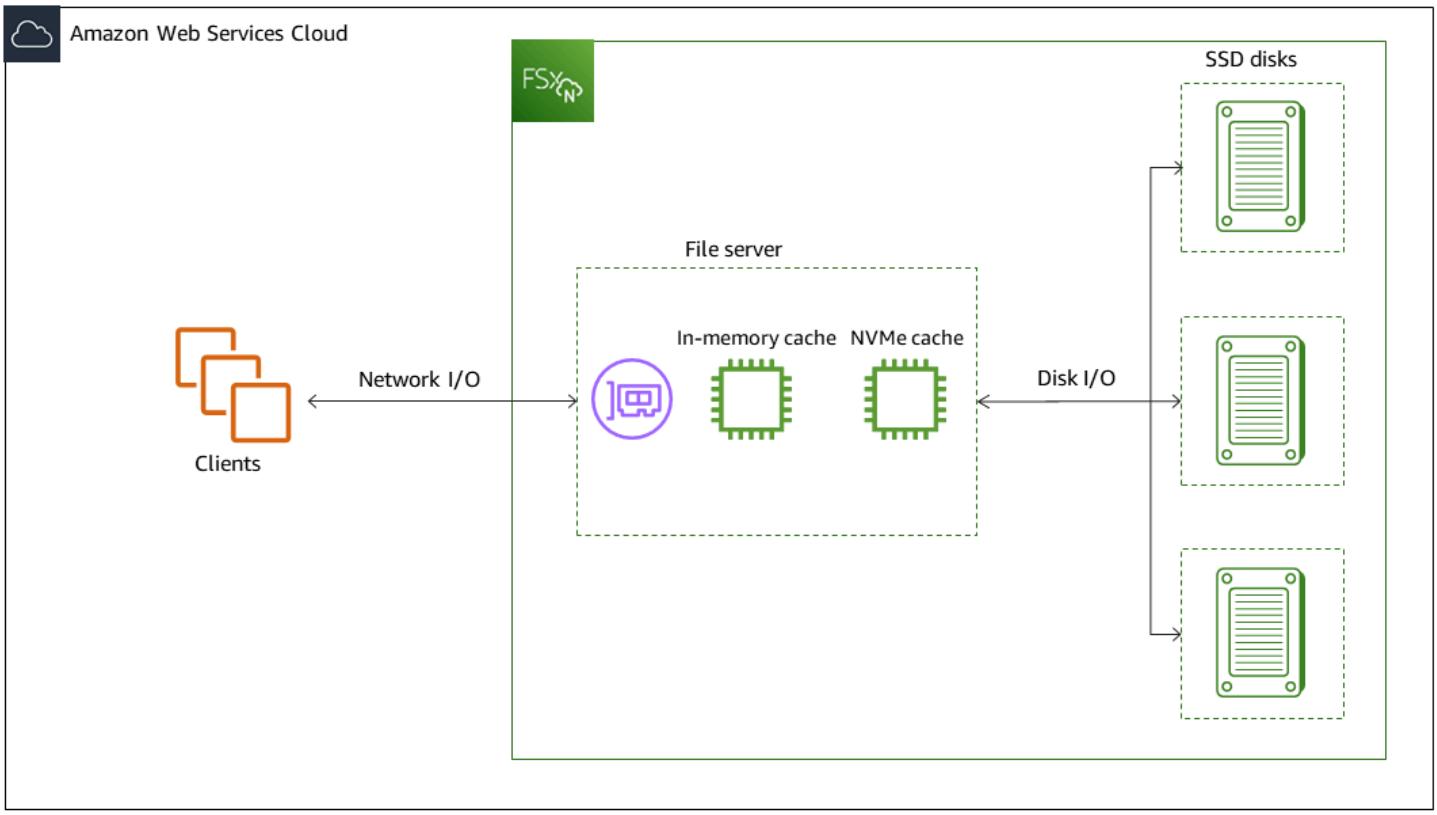
koneksi jaringan antara klien dan server secara bersamaan untuk agregat bandwidth jaringan untuk pemanfaatan maksimal. Untuk informasi tentang penggunaan NetApp ONTAP CLI untuk mengonfigurasi SMB Multichannel, lihat Mengonfigurasi Multichannel SMB untuk performa dan redundansi.

Klien NFS dapat menggunakan opsi `nconnect` mount untuk memiliki beberapa koneksi TCP (hingga 16) yang terkait dengan satu pemasangan NFS. Klien NFS semacam itu melakukan multipleks operasi file ke beberapa koneksi TCP secara round-robin dan dengan demikian memperoleh throughput yang lebih tinggi dari bandwidth jaringan yang tersedia. Dukungan NFSv3 dan NFSv4.1+. `nconnect` Bandwidth jaringan instans Amazon EC2 menjelaskan dupleks penuh 5 Gbps per batas bandwidth aliran jaringan. Anda dapat mengatasi batas ini dengan menggunakan beberapa aliran jaringan dengan `nconnect` atau SMB multichannel. Lihat dokumentasi klien NFS Anda untuk mengonfirmasi `nconnect` apakah didukung dalam versi klien Anda. Untuk informasi selengkapnya tentang NetApp ONTAP dukungan`nconnect`, lihat ONTAPdukungan untuk NFSv4.1.

Detail performa

Untuk memahami Amazon FSx untuk model kinerja NetApp ONTAP secara rinci, Anda dapat memeriksa komponen arsitektur sistem file Amazon FSx. Instans komputasi klien Anda, baik yang ada di dalam AWS maupun di tempat, mengakses sistem file Anda melalui satu atau beberapa antarmuka jaringan elastis (ENI). Antarmuka jaringan ini berada di Amazon VPC yang Anda kaitkan dengan sistem file Anda. Di belakang setiap sistem file ENI adalah NetApp ONTAP file server yang melayani data melalui jaringan ke klien yang mengakses sistem file. Amazon FSx menyediakan cache dalam memori yang cepat dan cache NVMe di setiap server file untuk meningkatkan kinerja data yang paling sering diakses. Terlampir ke setiap server file adalah disk SSD yang menghosting data sistem file Anda.

Komponen ini digambarkan dalam diagram berikut.



Sesuai dengan komponen arsitektur ini—antarmuka jaringan, cache dalam memori, cache NVMe, dan volume penyimpanan—adalah karakteristik kinerja utama Amazon FSx untuk sistem file NetApp ONTAP yang menentukan keseluruhan throughput dan kinerja IOPS.

- Performa I/O Jaringan: throughput/IOPS permintaan antara klien dan file server (secara agregat)
- Ukuran cache dalam memori dan NVMe pada server file: ukuran set kerja aktif yang dapat ditampung untuk caching
- Kinerja I/O Disk: Throughput/IOPS permintaan antara server file dan disk penyimpanan

Ada dua faktor yang menentukan karakteristik kinerja ini untuk sistem file Anda: jumlah total IOPS SSD dan kapasitas throughput yang Anda konfigurasikan untuk itu. Dua karakteristik kinerja pertama - kinerja I/O jaringan dan ukuran cache dalam memori dan NVMe - hanya ditentukan oleh kapasitas throughput, sedangkan yang ketiga - kinerja I/O disk - ditentukan oleh kombinasi kapasitas throughput dan SSD IOPS.

Beban kerja berbasis file biasanya runcing, ditandai dengan periode pendek dan intens I/O tinggi dengan banyak waktu idle antara semburan. Untuk mensupport beban kerja runcing, selain kecepatan dasar bahwa yang dapat dipertahankan sistem file 24/7, Amazon FSx menyediakan kemampuan untuk meledak hingga kecepatan yang lebih tinggi selama periode waktu untuk

operasi I/O jaringan dan disk I/O. Amazon FSx menggunakan mekanisme kredit I/O jaringan untuk mengalokasikan throughput dan IOPS berdasarkan pemanfaatan rata-rata - sistem file bertambah kredit ketika throughput dan penggunaan IOPS mereka di bawah batas dasar mereka, dan dapat menggunakan kredit ini ketika mereka melakukan operasi I/O.

Operasi tulis menggunakan bandwidth jaringan dua kali lebih banyak daripada operasi baca. Operasi tulis harus direplikasi pada server file sekunder, sehingga operasi penulisan tunggal menghasilkan dua kali jumlah throughput jaringan.

Dampak jenis penerapan pada kinerja

Anda dapat membuat dua jenis sistem file dengan FSx untuk ONTAP. Sistem file dengan sepasang server file ketersediaan tinggi (HA) tunggal disebut sistem file scale-up. Sistem file dengan beberapa pasangan HA disebut sistem file scale-out. Untuk informasi selengkapnya, lihat Pasangan ketersediaan tinggi (HA).

FSx untuk sistem file ONTAP Multi-AZ dan Single-AZ memberikan latensi operasi file sub-milidetik yang konsisten dengan penyimpanan SSD dan latensi puluhan milidetik dengan penyimpanan kolam kapasitas. Selain itu, sistem file yang memenuhi persyaratan berikut menyediakan cache baca NVMe untuk mengurangi latensi baca dan meningkatkan IOPS untuk data yang sering dibaca:

- Sistem file multi-AZ
- Sistem file penskalaan single-AZ dibuat setelah 28 November 2022 dengan kapasitas throughput minimal 2 GBps

Tabel berikut menunjukkan jumlah kapasitas throughput yang dapat ditingkatkan oleh sistem file tergantung pada faktor-faktor seperti jumlah pasangan ketersediaan tinggi (HA) dan Wilayah AWS ketersediaan.

Scale-up

Spesifikasi kinerja ini berlaku untuk sistem file scale-up.

Throughput maksimum dari penyimpanan SSD per pasangan HA untuk sistem file scale-up

	Wilayah Timur AS (Ohio), Wilayah AS Timur (Virginia N.), Wilayah Barat AS (Oregon), dan Eropa (Irlandia)		Semua Wilayah AWS tempat lain di mana FSx untuk ONTAP tersedia	
	Baca throughput (MBps)	Tulis throughput (MBps)	Baca throughput (MBps)	Tulis throughput (MBps)
Single-AZ	4,096*	1.000	2,048	750
Multi-AZ	4,096*	1.800	2,048	1.300

> **Note**
>
> * Untuk menyediakan kapasitas throughput 4 GBps, sistem file Anda harus dikonfigurasi dengan kapasitas penyimpanan SSD minimal 5.120 GiB dan 160.000 IOPS SSD.

Scale-out

Spesifikasi kinerja ini berlaku untuk sistem file scale-out.

Throughput maksimum dari penyimpanan SSD per pasangan HA untuk sistem file scale-out

	Baca throughput (MBps)	Tulis throughput (MBps)
Penskalaan AZ tunggal	6,144*	1.100*

> **Note**
>
> * Per pasangan HA (hingga 12). Untuk informasi selengkapnya, lihat Pasangan ketersediaan tinggi (HA).

Dampak kapasitas penyimpanan terhadap performa

Tingkat throughput dan IOPS disk maksimum tingkat yang dapat dicapai sistem file Anda lebih rendah dari:

- tingkat kinerja disk yang disediakan oleh server file Anda, berdasarkan kapasitas throughput yang Anda pilih untuk sistem file Anda
- tingkat kinerja disk yang disediakan oleh jumlah IOPS SSD yang Anda berikan untuk sistem file Anda

Secara default, penyimpanan SSD sistem file Anda menyediakan hingga tingkat throughput disk dan IOPS berikut:

- Throughput disk (MBps per TiB penyimpanan): 768
- Disk IOPS (IOP per TiB penyimpanan): 3.072

Dampak kapasitas throughput terhadap performa

Setiap sistem file Amazon FSx memiliki kapasitas throughput yang Anda konfigurasikan ketika sistem file dibuat. Kapasitas throughput sistem file Anda menentukan tingkat kinerja I/O jaringan, atau kecepatan di mana setiap server file yang menghosting sistem file Anda dapat melayani data file melalui jaringan ke klien yang mengaksesnya. Tingkat kapasitas throughput yang lebih tinggi datang dengan lebih banyak memori dan penyimpanan non-volatile memory express (NVMe) untuk caching data pada setiap server file, dan tingkat kinerja I/O disk yang lebih tinggi yang didukung oleh setiap server file.

Anda dapat secara opsional menyediakan tingkat IOPS SSD yang lebih tinggi saat membuat sistem file Anda. Tingkat maksimum SSD IOPS yang dapat dicapai oleh sistem file Anda juga ditentukan oleh kapasitas throughput sistem file Anda, bahkan ketika menyediakan IOPS SSD tambahan.

Tabel berikut menunjukkan set lengkap spesifikasi untuk kapasitas throughput, bersama dengan tingkat dasar dan burst, dan jumlah memori untuk caching pada server file yang sesuai. Wilayah AWS

Single-AZ (scale-up)

> Spesifikasi kinerja ini berlaku untuk sistem file penskalaan Single-AZ yang dibuat setelah 28 November 2022 dalam yang ditentukan. Wilayah AWS

Spesifikasi kinerja untuk sistem file sebagai berikut Wilayah AWS: AS Timur (Virginia N.), AS Timur (Ohio), AS Barat (Oregon), dan Eropa (Irlandia)

FSxkapasitas throughput (MBps)	Kapasitas throughput jaringan (MBps)		IOPS Jaringan	Caching dalam memori (GB)	NVMe membaca caching (GB)	Throughput disk (MBps)		Drive SSD IOPS *	
	Baseline	Meledak				Baseline	Meledak	Baseline	Meledak
128	188	1.500	Puluhan ribu baseline	16	–	128	1.250	6.000	40.000
256	375	1.500		32	–	256	1.250	12.000	40.000
512	750	1.500	Puluhan ribu baseline	64	–	512	1.250	20.000	40.000
1,024	1.500	–		128	–	1,024	1.250	40.000	–
2,048	3,125	–		256	1.900	2,048	–	80.000	–
4,096	6,250	–		512	5,400	4,096	–	160.000	–

> **Note**
>
> * IOPS SSD Anda hanya digunakan saat Anda mengakses data yang tidak di-cache di cache memori server file Anda atau cache NVMe.

Spesifikasi kinerja ini berlaku untuk sistem file penskalaan Single-AZ di semua sistem lain di mana Wilayah AWS FSx untuk ONTAP tersedia.

Spesifikasi kinerja untuk sistem file di semua lainnya di Wilayah AWS mana FSx untuk ONTAP tersedia

Kapasitas throughput FSx (MBps)	Kapasitas throughput jaringan (MBps)		IOPS Jaringan	Caching dalam memori (GB)	Throughput disk (MBps)		Drive SSD IOPS *	
	Baseline	Meledak			Baseline	Meledak	Baseline	Meledak
128	150	1.250	Puluhan ribu baseline	16	128	600	6.000	18,750
256	300	1.250		32	256	600	12.000	18,750
512	625	1.250	Puluhan ribu baseline	64	512	600	18,750	–
1,024	1.500	–		128	1,024	–	40.000	–
2,048	3,125	–		256	2,048	–	80.000	–

> **Note**
>
> * IOPS SSD Anda hanya digunakan saat Anda mengakses data yang tidak di-cache di cache memori server file Anda atau cache NVMe.

Single-AZ (scale-out)

Spesifikasi kinerja ini berlaku untuk sistem file scale-out.

Spesifikasi kinerja untuk sistem file scale-out

Kapasitas throughput FSx (MBps)	Kapasitas throughput jaringan (MBps)		IOPS Jaringan	Caching dalam memori (GB)	Throughput disk (MBps)		Drive SSD IOPS *	
	Baseline	Meledak			Baseline	Meledak	Baseline	Meledak

Kapasitas throughput FSx (MBps)	Kapasitas throughput jaringan (MBps)		IOPS Jaringan	Caching dalam memori (GB)	Throughput disk (MBps)		Drive SSD IOPS *	
3,072**	6,250	–	Puluhan ribu baseline	128	3,072	–	100.000	–
6,144**	12.500	–		256	6,144	–	200.000	–

> **Note**
>
> * IOPS SSD Anda hanya digunakan saat Anda mengakses data yang tidak di-cache di cache memori server file Anda atau cache NVMe.
> ** Per pasangan HA (hingga 12). Untuk informasi selengkapnya, lihat Pasangan ketersediaan tinggi (HA).

Multi-AZ (scale-up)

Spesifikasi kinerja ini berlaku untuk sistem file penskalaan Multi-AZ yang dibuat setelah 28 November 2022 dalam yang ditentukan. Wilayah AWS

Spesifikasi kinerja untuk sistem file sebagai berikut Wilayah AWS: AS Timur (Virginia N.), AS Timur (Ohio), AS Barat (Oregon), dan Eropa (Irlandia)

Kapasitas throughput FSx (MBps)	Kapasitas throughput jaringan (MBps)		IOPS Jaringan	Caching dalam memori (GB)	Caching NVMe (GB)	Throughput disk (MBps)		Drive SSD IOPS *	
	Baseline	Meledak				Baseline	Meledak	Baseline	Meledak
128	188	1.500	Puluhan ribu baseline	16	238	128	1.250	6.000	40.000
256	375	1.500		32	475	256	1.250	12.000	40.000

Kapasitas throughput FSx (MBps)	Kapasitas throughput jaringan (MBps)		IOPS Jaringan	Caching dalam memori (GB)	Caching NVMe (GB)	Throughput disk (MBps)		Drive SSD IOPS *	
512	750	1.500	Puluhan ribu baseline	64	950	512	1.250	20.000	40.000
1,024	1.500	–		128	1.900	1,024	1.250	40.000	–
2,048	3,125	–		256	3,800	2,048	–	80.000	–
4,096	6,250	–		512	7,600	4,096	–	160.000	–

> **Note**
>
> * IOPS SSD Anda hanya digunakan saat Anda mengakses data yang tidak di-cache di cache memori server file Anda atau cache NVMe.

Spesifikasi kinerja ini berlaku untuk sistem file penskalaan Multi-AZ di semua sistem lain di mana Wilayah AWS FSx untuk ONTAP tersedia.

Spesifikasi kinerja untuk sistem file di semua lainnya di Wilayah AWS mana FSx untuk ONTAP tersedia

Kapasitas throughput FSx (MBps)	Kapasitas throughput jaringan (MBps)		IOPS Jaringan	Caching dalam memori (GB)	Caching NVMe (GB)	Throughput disk (MBps)		Drive SSD IOPS *	
	Baseline	Meledak				Baseline	Meledak	Baseline	Meledak
128	150	1.250	Puluhan ribu baseline	16	150	128	600	6.000	18,750
256	300	1.250		32	300	256	600	12.000	18,750
512	625	1.250	Puluhan ribu baseline	64	600	512	600	18,750	–
1,024	1.500	–		128	1.200	1,024	–	40.000	–

Kapasitas throughput FSx (MBps)	Kapasitas throughput jaringan (MBps)		IOPS Jaringan	Caching dalam memori (GB)	Caching NVMe (GB)	Throughput disk (MBps)		Drive SSD IOPS *	
2,048	3,125	–		256	2,400	2,048	–	80.000	–

> **Note**
>
> * IOPS SSD Anda hanya digunakan saat Anda mengakses data yang tidak di-cache di cache memori server file Anda atau cache NVMe.

Contoh: kapasitas penyimpanan dan kapasitas throughput

Contoh berikut menggambarkan bagaimana kapasitas penyimpanan dan kapasitas throughput berdampak pada performa sistem file.

Sistem file scale-up yang dikonfigurasi dengan kapasitas penyimpanan SSD 2 TiB dan kapasitas throughput 512 MBps memiliki tingkat throughput berikut:

- Throughput jaringan — baseline 625 MBps dan burst 1.250 MBps (lihat tabel kapasitas throughput)
- Throughput disk — 512 MBps baseline dan 600 MBps burst.

Beban kerja Anda yang mengakses sistem file akan dapat mendorong hingga 625 MBps baseline dan 1.250 MBps burst throughput untuk operasi file yang dilakukan pada data yang diakses secara aktif yang di-cache di cache file server dalam memori dan cache NVMe.

Mengelola FSx untuk sumber daya ONTAP

Menggunakan AWS Management Console, AWS CLI, dan ONTAP CLI dan API, Anda dapat melakukan tindakan administratif berikut untuk fsX untuk sumber daya ONTAP:

- Membuat, mencantumkan, memperbarui, dan menghapus sistem file, penyimpanan mesin virtual (SVM), volume, cadangan, dan tag.
- Mengelola akses, akun administratif dan kata sandi, persyaratan kata sandi, protokol SMB dan iSCSI, aksesibilitas jaringan untuk target pemasangan sistem file yang ada

Topik

Mengelola fsX untuk sistem file ONTAP

Sistem file adalah sumber daya Amazon FSx utama, analog dengan kluster ONTAP lokal. Anda menentukan kapasitas penyimpanan solid state drive (SSD) dan kapasitas throughput untuk sistem file Anda, dan memilih virtual private cloud (VPC) untuk membuat sistem file. Setiap sistem file

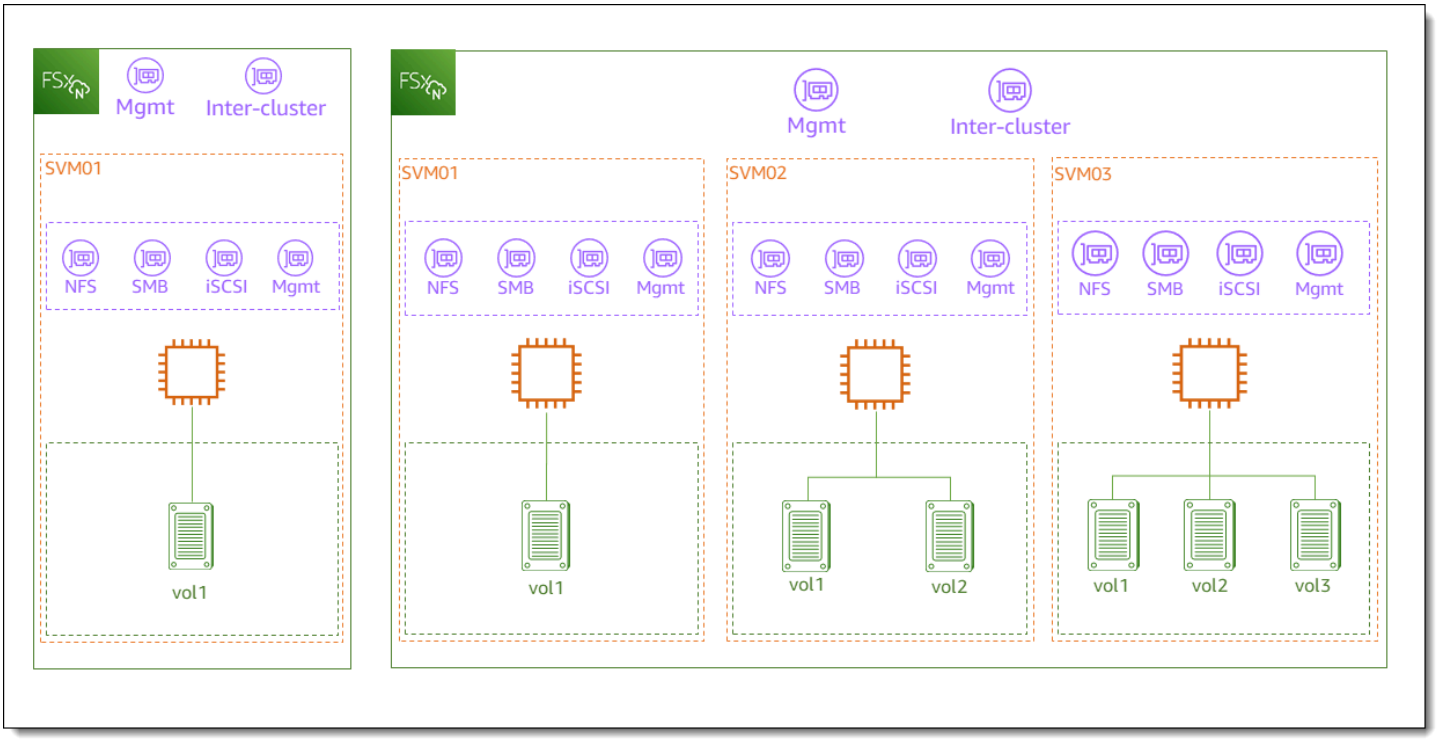
memiliki endpoint manajemen yang dapat Anda gunakan untuk mengelola sumber daya dan data dengan ONTAP CLI atau REST API.

Sumber daya sistem file

Sistem file Amazon FSx untuk NetApp ONTAP terdiri dari sumber daya utama berikut:

- Perangkat keras fisik dari sistem file itu sendiri, yang mencakup server file dan media penyimpanan.
- Satu atau lebih pasangan server file (HA) yang sangat tersedia, yang menghosting mesin virtual penyimpanan (SVM) Anda. Sistem file scale-up memiliki satu pasangan HA, dan sistem file scale-out memiliki dua atau lebih pasangan HA. Setiap pasangan HA memiliki kolam penyimpanan yang disebut agregat. Kumpulan agregat di semua pasangan HA membentuk tingkat penyimpanan SSD Anda.
- Satu atau lebih mesin virtual penyimpanan (SVM) yang meng-host volume sistem file dan memiliki kredensialnya sendiri dan manajemen akses.
- Satu atau lebih volume yang secara virtual mengatur data Anda dan dipasang oleh klien Anda.

Gambar berikut mengilustrasikan arsitektur FSx skala untuk sistem file ONTAP dengan satu pasangan HA, dan hubungan antara sumber daya utamanya. FSx untuk sistem file ONTAP di sebelah kiri adalah sistem file paling sederhana, dengan satu SVM dan satu volume. Sistem file di sebelah kanan memiliki beberapa SVM, dengan beberapa SVM memiliki banyak volume. Sistem file dan SVM masing-masing memiliki beberapa titik akhir manajemen, dan SVM juga memiliki titik akhir akses data.



Saat membuat fsX untuk sistem file ONTAP, Anda menentukan properti berikut:

- Jenis penyebaran — Jenis penyebaran sistem file Anda (Multi-AZ atau Single-AZ). Sistem file single-AZ mereplikasi data Anda dan menawarkan failover otomatis dalam satu Availability Zone, dan menawarkan sistem file scale-out. Sistem file multi-AZ memberikan ketahanan tambahan dengan juga mereplikasi data Anda dan mendukung failover di beberapa Availability Zone dalam hal yang sama. Wilayah AWS
- Kapasitas penyimpanan — Ini adalah jumlah penyimpanan SSD, hingga 192 tebibytes (TiB) untuk sistem file scale-up dan 1 pebibyte (PiB) untuk sistem file scale-out.
- SSD IOPS — Secara default, setiap gigabyte penyimpanan SSD mencakup tiga IOPS SSD (hingga maksimum yang didukung oleh konfigurasi sistem file Anda). Anda dapat secara opsional menyediakan IOPS SSD tambahan sesuai kebutuhan.
- Kapasitas throughput — Kecepatan berkelanjutan di mana server file dapat melayani data.
- Networking — VPC dan subnet untuk endpoint manajemen dan akses data yang dibuat oleh sistem file Anda. Untuk sistem file multi-AZ, Anda juga menentukan rentang alamat IP dan tabel rute.
- Enkripsi — Kunci AWS Key Management Service (AWS KMS) yang digunakan untuk mengenkripsi data sistem file saat istirahat.

- Akses administratif — Anda dapat menentukan kata sandi untuk `fsxadmin` pengguna. Anda dapat menggunakan pengguna ini untuk mengelola sistem file dengan menggunakan NetApp ONTAP CLI dan REST API.

Anda dapat mengelola fsX untuk sistem file ONTAP dengan menggunakan ONTAP NetApp CLI atau REST API. Anda juga dapat mengatur SnapMirror atau SnapVault hubungan antara sistem file Amazon FSx dan penyebaran ONTAP lainnya (termasuk sistem file Amazon FSx lainnya). Setiap fsX untuk sistem file ONTAP memiliki titik akhir sistem file berikut yang menyediakan akses ke aplikasi: NetApp

- Manajemen — Gunakan endpoint ini untuk mengakses NetApp ONTAP CLI melalui Secure Shell (SSH), atau untuk menggunakan NetApp ONTAP REST API dengan sistem file Anda.
- Intercluster — Gunakan titik akhir ini saat mengatur replikasi menggunakan NetApp SnapMirror atau menggunakan caching. NetApp FlexCache

Untuk informasi selengkapnya, lihat Mengelola FSx untuk sumber daya ONTAP menggunakan aplikasi NetApp dan Replikasi terjadwal menggunakan NetApp SnapMirror.

Pasangan ketersediaan tinggi (HA)

Setiap fsX untuk sistem file ONTAP didukung oleh satu atau beberapa pasangan server file ketersediaan tinggi (HA) dalam konfigurasi siaga aktif. Dalam konfigurasi ini, ada server file pilihan yang secara aktif melayani lalu lintas dan server file sekunder yang mengambil alih jika server aktif tidak tersedia. FSx untuk sistem file scale-up ONTAP didukung oleh satu pasangan HA, yang memberikan kapasitas throughput hingga 4 GBps dan 160.000 IOP SSD. FSx untuk sistem file scale-out ONTAP didukung oleh hingga 12 pasang HA, yang dapat menghasilkan kapasitas throughput hingga 72 GBps dan 2.400.000 IOPS SSD (kapasitas throughput 6 GBps dan 200.000 IOPS SSD per pasangan HA).

Saat Anda membuat sistem file dari konsol Amazon FSx, Amazon FSx merekomendasikan jumlah pasangan HA yang harus Anda gunakan berdasarkan penyimpanan SSD yang Anda inginkan. Anda juga dapat secara manual memilih jumlah pasangan HA berdasarkan beban kerja dan persyaratan kinerja Anda. Kami menyarankan Anda menggunakan satu pasangan HA jika persyaratan sistem file Anda dipenuhi dengan kapasitas throughput hingga 4 GBps dan 160.000 IOP SSD, dan beberapa pasangan HA jika beban kerja Anda membutuhkan tingkat skalabilitas kinerja yang lebih tinggi.

Setiap pasangan HA memiliki satu agregat, yang merupakan kumpulan disk fisik yang logis.

> **Note**
>
> Anda tidak dapat menambahkan pasangan HA ke sistem file yang ada. Sebagai gantinya, Anda dapat memigrasikan data antar sistem file (dengan pasangan HA yang berbeda) menggunakan SnapMirror AWS DataSync,, atau dengan memulihkan data Anda dari cadangan ke sistem file baru.

Membuat fsX untuk sistem file ONTAP

Bagian ini menjelaskan cara membuat fsX untuk sistem file ONTAP menggunakan konsol Amazon FSx,, atau Amazon FSx AWS CLI API. Anda dapat membuat sistem file di cloud pribadi virtual (VPC) yang Anda miliki, atau di VPC yang Akun AWS telah dibagikan orang lain dengan Anda. Ada pertimbangan saat membuat sistem file multi-AZ di VPC di mana Anda adalah peserta. Pertimbangan ini dijelaskan dalam topik ini.

Secara default, saat Anda membuat sistem file baru dari konsol Amazon FSx, Amazon FSx secara otomatis membuat sistem file dengan mesin virtual penyimpanan tunggal (SVM) dan satu volume, memungkinkan akses cepat ke data dari instance Linux melalui protokol Sistem File Jaringan (NFS). Saat membuat sistem file, Anda dapat secara opsional menggabungkan SVM ke Active Directory untuk mengaktifkan akses dari klien Windows dan macOS melalui protokol Server Message Block (SMB). Setelah sistem file Anda dibuat, Anda dapat membuat SVM dan volume tambahan sesuai kebutuhan.

Untuk membuat sistem file (konsol)

Prosedur ini menggunakan opsi pembuatan pembuatan Standar untuk membuat fsX untuk sistem file ONTAP dengan konfigurasi yang Anda sesuaikan untuk kebutuhan Anda. Untuk informasi tentang menggunakan opsi Pembuatan cepat untuk membuat sistem file dengan cepat dengan set parameter konfigurasi default, lihatLangkah 1: Buat Amazon FSx untuk sistem file NetApp ONTAP.

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Di dasbor, pilih Buat sistem file.
3. Pada halaman Pilih jenis sistem file, untuk opsi sistem File, pilih Amazon FSx untuk NetApp ONTAP, lalu pilih Berikutnya.
4. Di bagian Metode pembuatan, pilih Standar buat.
5. Di bagian Detail sistem file, berikan informasi berikut:

- Untuk nama sistem File - opsional, masukkan nama untuk sistem file Anda. Lebih mudah untuk menemukan dan mengelola sistem file Anda ketika Anda menamainya. Anda dapat menggunakan maksimal 256 huruf Unicode, spasi putih, dan angka, ditambah karakter khusus ini: + - =. _:/
- Untuk Jenis Deployment Pilih Multi-AZ atau Single-AZ.
  - Sistem file multi-AZ mereplikasi data Anda dan mendukung failover di beberapa Availability Zone secara bersamaan. Wilayah AWS
  - Sistem file single-AZ mereplikasi data Anda dan menawarkan failover otomatis dalam satu Availability Zone.

    > **Note**
    >
    > Pilih Single-AZ jika Anda menginginkan opsi untuk membuat sistem file dengan dua atau lebih pasangan ketersediaan tinggi (HA) (hingga 12). Untuk informasi selengkapnya, lihat Pasangan ketersediaan tinggi (HA).

  Untuk informasi selengkapnya, lihat Ketersediaan dan daya tahan.
- Untuk kapasitas penyimpanan SSD, masukkan kapasitas penyimpanan sistem file Anda, dalam gibibytes (GiB). Masukkan bilangan bulat dalam kisaran 1.048-1.048.576 GiB (hingga 1 pebibyte [PiB]).

  Anda dapat meningkatkan jumlah kapasitas penyimpanan sesuai kebutuhan setiap saat setelah Anda membuat sistem file. Untuk informasi selengkapnya, lihat Mengelola kapasitas penyimpanan.
- Untuk Provisioned SSD IOPS, Anda memiliki dua opsi untuk menyediakan jumlah IOPS untuk sistem file Anda:
  - Pilih Otomatis (default) jika Anda ingin Amazon FSx secara otomatis menyediakan 3 IOPS per GiB penyimpanan SSD.
  - Pilih User-provisioned jika Anda ingin menentukan jumlah IOPS. Anda dapat menyediakan maksimum 200.000 IOPS SSD per sistem file.

    > **Note**
    >
    > Anda dapat meningkatkan IOPS SSD yang disediakan setelah Anda membuat sistem file. Perlu diingat bahwa tingkat maksimum SSD IOPS yang dapat dicapai sistem

file Anda juga ditentukan oleh kapasitas throughput sistem file Anda bahkan ketika menyediakan IOPS SSD tambahan. Untuk informasi selengkapnya, lihat Dampak kapasitas throughput terhadap performa dan Mengelola kapasitas penyimpanan.

- Untuk kapasitas Throughput, Anda memiliki dua opsi untuk menentukan kapasitas throughput Anda dalam megabyte per detik (MBps):
  - Pilih Kapasitas throughput yang disarankan jika Anda ingin Amazon FSx secara otomatis memilih kapasitas throughput berdasarkan jumlah kapasitas penyimpanan yang Anda pilih.
  - Pilih Tentukan kapasitas throughput jika Anda ingin menentukan jumlah kapasitas throughput. Jika Anda memilih opsi ini, dropdown kapasitas Throughput akan muncul dan diisi berdasarkan jenis penerapan yang Anda pilih. Anda juga dapat memilih jumlah pasangan HA (hingga 12). Untuk informasi selengkapnya, lihat Pasangan ketersediaan tinggi (HA).

  Kapasitas throughput adalah kecepatan berkelanjutan di mana server file yang menyimpan sistem file Anda dapat melayani data. Untuk informasi selengkapnya, lihat Amazon FSx untuk NetApp kinerja ONTAP.

6. Di bagian Jaringan, berikan informasi berikut:

- Untuk Virtual Private Cloud (VPC), pilih VPC yang ingin Anda kaitkan dengan sistem file Anda.
- Untuk Grup Keamanan VPC, Anda dapat memilih grup keamanan untuk dikaitkan dengan antarmuka jaringan sistem file Anda. Jika Anda tidak menentukannya, Amazon FSx akan mengaitkan grup keamanan default VPC dengan sistem file Anda.
- Tentukan Subnet untuk server file Anda. Jika Anda membuat sistem file Multi-AZ, pilih juga subnet Siaga untuk server file siaga.
- (Hanya multi-AZ) Untuk tabel rute VPC, tentukan tabel rute VPC untuk membuat titik akhir sistem file Anda. Pilih semua tabel rute VPC yang terkait dengan subnet tempat klien Anda berada. Secara default, Amazon FSx memilih tabel rute default VPC Anda. Untuk informasi selengkapnya, lihat Mengakses data dari luar VPC penyebaran.

> **Note**
>
> Amazon FSx mengelola tabel rute ini untuk sistem file multi-AZ menggunakan otentikasi berbasis tag. Tabel rute ini ditandai dengan`Key: AmazonFSx; Value: ManagedByAmazonFSx`. Saat membuat FSx untuk sistem file ONTAP Multi-AZ

menggunakan AWS CloudFormation kami sarankan Anda menambahkan tag secara manual. `Key: AmazonFSx; Value: ManagedByAmazonFSx`

- (Hanya multi-AZ) Rentang alamat IP titik akhir menentukan rentang alamat IP di mana titik akhir untuk mengakses sistem file Anda dibuat.

  Anda memiliki tiga opsi untuk rentang alamat IP titik akhir:

  - Rentang alamat IP yang tidak dialokasikan dari VPC Anda - Amazon FSx memilih 64 alamat IP terakhir dari rentang CIDR utama VPC untuk digunakan sebagai rentang alamat IP titik akhir untuk sistem file. Rentang ini dibagi di beberapa sistem file jika Anda memilih opsi ini beberapa kali.

    > **Note**
    >
    > Opsi ini berwarna abu-abu jika salah satu dari 64 alamat IP terakhir dalam rentang CIDR utama VPC digunakan oleh subnet. Dalam hal ini, Anda masih dapat memilih rentang alamat in-VPC (yaitu, rentang yang tidak berada di akhir rentang CIDR utama Anda atau rentang yang ada di CIDR sekunder VPC Anda) dengan memilih opsi Masukkan rentang alamat IP.

  - Untuk subnet Pilihan, tentukan Subnet untuk server file Anda. Jika Anda membuat sistem file Multi-AZ, pilih juga subnet Siaga untuk server file siaga.
  - (Hanya multi-AZ) Untuk tabel rute VPC, tentukan tabel rute VPC untuk membuat titik akhir sistem file Anda. Pilih semua tabel rute VPC yang terkait dengan subnet tempat klien Anda berada. Secara default, Amazon FSx memilih tabel rute default VPC Anda.
  - (Hanya multi-AZ) Rentang alamat IP titik akhir menentukan rentang alamat IP di mana titik akhir untuk mengakses sistem file Anda dibuat.

    Anda memiliki tiga opsi untuk rentang alamat IP titik akhir:

    - Rentang alamat IP yang tidak dialokasikan dari VPC Anda - Amazon FSx memilih 64 alamat IP terakhir dari rentang CIDR utama VPC untuk digunakan sebagai rentang alamat IP titik akhir untuk sistem file. Rentang ini dibagi di beberapa sistem file jika Anda memilih opsi ini beberapa kali.

> **Note**
>
> Opsi ini berwarna abu-abu jika salah satu dari 64 alamat IP terakhir dalam rentang CIDR utama VPC digunakan oleh subnet. Dalam hal ini, Anda masih dapat memilih rentang alamat in-VPC (yaitu, rentang yang tidak berada di akhir rentang CIDR utama Anda atau rentang yang ada di CIDR sekunder VPC Anda) dengan memilih opsi Masukkan rentang alamat IP.

- Rentang alamat IP mengambang di luar VPC Anda - Amazon FSx memilih rentang alamat 198.19.x.0/24 yang belum digunakan oleh sistem file lain dengan VPC dan tabel rute yang sama.
- Masukkan rentang alamat IP — Anda dapat memberikan rentang CIDR yang Anda pilih sendiri. Rentang alamat IP yang Anda pilih dapat berada di dalam atau di luar rentang alamat IP VPC, asalkan tidak tumpang tindih dengan subnet apa pun.

> **Note**
>
> Jangan memilih rentang apa pun yang termasuk dalam rentang CIDR berikut, karena tidak kompatibel dengan FSx untuk ONTAP:
>
> - 0.0.0.0/8
> - 127.0.0.0/8
> - 198.19.0.0/20
> - 224.0.0.0/4
> - 240.0.0.0/4
> - 255.255.255.255/32

7. Di bagian Keamanan & enkripsi, untuk kunci Enkripsi, pilih kunci enkripsi AWS Key Management Service (AWS KMS) yang melindungi data sistem file Anda saat istirahat.
8. Untuk kata sandi administratif sistem file, masukkan kata sandi aman untuk `fsxadmin` pengguna. Konfirmasikan kata sandi.

   Anda dapat menggunakan `fsxadmin` pengguna untuk mengelola sistem file Anda menggunakan ONTAP CLI dan REST API. Untuk informasi selengkapnya tentang `fsxadmin` pengguna, lihatMengelola sistem file dengan ONTAP CLI.
9. Di bagian konfigurasi mesin virtual penyimpanan default, berikan informasi berikut:

- Di bidang nama mesin virtual Penyimpanan, berikan nama untuk mesin virtual penyimpanan. Anda dapat menggunakan maksimal 47 karakter alfanumerik, ditambah karakter khusus garis bawah (_).
- Untuk kata sandi administratif SVM, Anda dapat memilih Tentukan kata sandi dan berikan kata sandi untuk pengguna SVM. `vsadmin` Anda dapat menggunakan `vsadmin` pengguna untuk mengelola SVM menggunakan ONTAP CLI atau REST API. Untuk informasi selengkapnya tentang `vsadmin` pengguna, lihatMengelola SVM dengan CLI ONTAP.

  Jika Anda memilih Jangan tentukan kata sandi (default), Anda masih dapat menggunakan `fsxadmin` pengguna sistem file untuk mengelola sistem file Anda menggunakan ONTAP CLI atau REST API, tetapi Anda tidak dapat menggunakan pengguna SVM Anda untuk melakukan `vsadmin` hal yang sama.
- Di bagian Active Directory, Anda dapat bergabung dengan Active Directory ke SVM. Untuk informasi selengkapnya, lihat Bekerja dengan Microsoft Active Directory di FSx untuk ONTAP.

  Jika Anda tidak ingin bergabung dengan SVM Anda ke Active Directory, pilih Jangan bergabung dengan Active Directory.

  Jika Anda ingin menggabungkan SVM Anda ke domain Active Directory yang dikelola sendiri, pilih Bergabung dengan Active Directory, dan berikan detail berikut untuk Active Directory Anda:
  - Nama NetBIOS dari objek komputer Active Directory yang akan dibuat untuk SVM Anda. Nama NetBIOS tidak boleh melebihi 15 karakter.
  - Nama domain yang memenuhi syarat dari Direktori Aktif Anda. Nama domain tidak boleh melebihi 255 karakter.
  - Alamat IP server DNS — Alamat IPv4 dari server Domain Name System (DNS) untuk domain Anda.
  - Nama pengguna akun layanan — Nama pengguna akun layanan di Direktori Aktif Anda yang ada. Jangan masukkan sebuah prefiks atau sufiks domain.
  - Kata sandi akun layanan — Kata sandi untuk akun layanan.
  - Konfirmasi kata sandi — Kata sandi untuk akun layanan.
  - (Opsional) Unit Organisasi (OU) - Nama jalur yang dibedakan dari unit organisasi tempat Anda ingin bergabung dengan sistem file Anda.
  - Grup administrator sistem file yang didelegasikan — Nama grup di Direktori Aktif Anda yang dapat mengelola sistem file Anda.

Jika Anda menggunakan AWS Managed Microsoft AD, Anda perlu menentukan grup seperti Administrator FSx AWS Delegasi, Administrator Delegasi AWS , atau grup kustom dengan izin yang didelegasikan ke OU.

Jika Anda bergabung dengan iklan yang dikelola sendiri, gunakan nama grup di iklan Anda. Grup default adalah`Domain Admins`.

10. Di bagian konfigurasi volume default, berikan informasi berikut untuk volume default yang dibuat dengan sistem file Anda:

    - Di bidang Nama volume, berikan nama untuk volume. Anda dapat menggunakan hingga 203 karakter alfanumerik atau garis bawah (_).
    - (Scale-up sistem file saja) Untuk gaya Volume, pilih salah satu FlexVolatau FlexGroup. FlexVolvolume adalah volume tujuan umum yang dapat mencapai 300 TiB dalam ukuran. FlexGroupvolume ditujukan untuk beban kerja berkinerja tinggi dan dapat berukuran hingga 20 PiB.
    - Untuk ukuran Volume, masukkan bilangan bulat apa pun dalam kisaran 800 gibibyte (GiB) — 2.000 pebibyte (PiB).
    - Untuk tipe Volume, pilih Read-Write (RW) untuk membuat volume yang dapat dibaca dan ditulis atau Perlindungan Data (DP) untuk membuat volume yang hanya-baca dan dapat digunakan sebagai tujuan hubungan atau. NetApp SnapMirror SnapVault Untuk informasi selengkapnya, lihat Tipe volume.
    - Untuk jalur Junction, masukkan lokasi di dalam sistem file untuk me-mount volume. Nama harus memiliki garis miring ke depan, misalnya`/vol3`.
    - Untuk efisiensi Penyimpanan, pilih Diaktifkan untuk mengaktifkan fitur efisiensi penyimpanan ONTAP (deduplikasi, kompresi, dan pemadatan). Untuk informasi selengkapnya, lihat fsX untuk efisiensi penyimpanan ONTAP.
    - Untuk gaya keamanan Volume, pilih antara Unix (Linux), NTFS, dan Mixed untuk volume. Untuk informasi selengkapnya, lihat Gaya keamanan volume.
    - Untuk kebijakan Snapshot, pilih kebijakan snapshot untuk volume. Untuk informasi selengkapnya tentang kebijakan snapshot, lihatKebijakan snapshot.

      Jika memilih Kebijakan khusus, Anda harus menentukan nama kebijakan di bidang kebijakan khusus. Kebijakan kustom harus sudah ada di SVM atau di sistem file. Anda dapat membuat kebijakan snapshot khusus dengan ONTAP CLI atau REST API. Untuk informasi selengkapnya, lihat Membuat Kebijakan Snapshot di Dokumentasi Produk NetApp ONTAP.

11. Di bagian Tingkatan penyimpanan volume default, untuk kebijakan tingkatan kumpulan Kapasitas, pilih kebijakan tiering kumpulan penyimpanan untuk volume, yang dapat berupa Otomatis (default), Hanya Snapshot, Semua, atau Tidak Ada. Untuk informasi selengkapnya tentang kebijakan tingkatan kumpulan kapasitas, lihatKebijakan tingkatan volume.

    Untuk periode pendinginan kebijakan Tiering, jika Anda telah menetapkan tingkat penyimpanan ke salah satu kebijakan `Auto` dan `Snapshot-only` kebijakan. Nilai yang valid adalah 2-183 hari. Periode pendinginan kebijakan tingkat volume menentukan jumlah hari sebelum data yang belum diakses ditandai dingin dan dipindahkan ke penyimpanan kolam kapasitas.

12. Di Backup dan pemeliharaan - opsional, Anda dapat mengatur opsi berikut:

    - Untuk pencadangan otomatis harian, pilih Diaktifkan untuk pencadangan harian otomatis. Pengaturan ini diaktifkan secara default.
    - Untuk jendela pencadangan otomatis Harian, atur waktu hari di Coordinated Universal Time (UTC) yang Anda inginkan untuk memulai jendela pencadangan otomatis harian. Window adalah 30 menit mulai dari waktu yang ditentukan ini. Window tidak dapat menindih Window cadangan pemeliharaan mingguan.
    - Untuk periode retensi cadangan otomatis, tetapkan periode dari 1—90 hari yang ingin Anda pertahankan pencadangan otomatis.
    - Untuk jendela pemeliharaan Mingguan, Anda dapat mengatur waktu dalam seminggu yang Anda inginkan untuk memulai jendela pemeliharaan. Hari 1 adalah Senin, 2 adalah Selasa, dan seterusnya. Window adalah 30 menit mulai dari waktu yang ditentukan ini. Window ini tidak dapat menindih window cadangan otomatis harian.

13. Untuk Tag - opsional, Anda dapat memasukkan kunci dan nilai untuk menambahkan tag ke sistem file Anda. Tag adalah pasangan nilai-kunci yang peka huruf besar-kecil yang membantu Anda mengelola, mem-filter, dan mencari sistem file Anda.

    Pilih Selanjutnya.

14. Tinjau konfigurasi sistem file yang ditampilkan pada halaman Buat sistem file. Untuk referensi Anda, perhatikan pengaturan sistem file mana yang dapat Anda modifikasi setelah sistem file dibuat.

15. Pilih Buat sistem file.

Untuk membuat sistem file (CLI)

- Untuk membuat FSx untuk sistem file ONTAP, gunakan perintah CLI create-file-system (atau operasi API CreateFileSistem yang setara), seperti yang ditunjukkan pada contoh berikut.

```
aws fsx create-file-system \
    --file-system-type ONTAP \
    --storage-capacity 1024 \
    --storage-type SSD \
    --security-group-ids security-group-id \

    --subnet-ids subnet-abcdef1234567890b subnet-abcdef1234567890c \
    --ontap-configuration DeploymentType=MULTI_AZ_1,
        ThroughputCapacity=512,PreferredSubnetId=subnet-abcdef1234567890b
```

Setelah berhasil membuat sistem file, Amazon FSx mengembalikan deskripsi sistem file dalam format JSON seperti yang ditunjukkan pada contoh berikut.

```
{
  "FileSystem": {
    "OwnerId": "111122223333",
    "CreationTime": 1625066825.306,
    "FileSystemId": "fs-0123456789abcdef0",
    "FileSystemType": "ONTAP",
    "Lifecycle": "CREATING",
    "StorageCapacity": 1024,
    "StorageType": "SSD",
    "VpcId": "vpc-11223344556677aab",
    "SubnetIds": [
      "subnet-abcdef1234567890b",
      "subnet-abcdef1234567890c"
    ],
    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "ResourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/
fs-0123456789abcdef0",
    "Tags": [],
    "OntapConfiguration": {
      "DeploymentType": "MULTI_AZ_HA_1",
      "EndpointIpAddressRange": "198.19.0.0/24",
      "Endpoints": {
```

```
        "Management": {
          "DnsName": "management.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
        },
        "Intercluster": {
          "DnsName": "intercluster.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
        }
      },
      "DiskIopsConfiguration": {
                "Mode": "AUTOMATIC",
                "Iops": 3072
      },
      "PreferredSubnetId": "subnet-abcdef1234567890b",
      "RouteTableIds": [
        "rtb-abcdef1234567890e",
        "rtb-abcd1234ef567890b"
      ],
      "ThroughputCapacity": 512,
      "WeeklyMaintenanceStartTime": "4:10:00"
    }
  }
}
```

> **Note**
>
> Berbeda dengan proses pembuatan sistem file di konsol, perintah `create-file-system` CLI dan operasi `CreateFileSystem` API tidak membuat SVM atau volume default. Untuk membuat SVM, lihatMembuat mesin virtual penyimpanan; untuk membuat volume, lihatMembuat volume.

Membuat fsX untuk sistem file ONTAP di subnet bersama

Berbagi VPC memungkinkan beberapa Akun AWS untuk membuat sumber daya ke dalam cloud pribadi virtual (VPC) bersama yang dikelola secara terpusat. Dalam model ini, akun yang memiliki VPC (pemilik) berbagi satu atau lebih subnet dengan akun lain (peserta) yang termasuk dalam organisasi yang sama dari. AWS Organizations

Akun peserta dapat membuat FSx untuk sistem file ONTAP Single-AZ dan Multi-AZ dalam subnet VPC yang telah dibagikan oleh akun pemilik dengan mereka. Agar akun peserta dapat membuat sistem file multi-AZ, akun pemilik juga perlu memberikan izin Amazon FSx untuk mengubah tabel

rute di subnet bersama atas nama akun peserta. Untuk informasi selengkapnya, lihat Mengelola dukungan VPC bersama untuk sistem file multi-AZ.

> **Note**
>
> Merupakan tanggung jawab akun peserta untuk berkoordinasi dengan pemilik VPC untuk mencegah pembuatan subnet VPC berikutnya yang akan tumpang tindih dengan CIDR in-VPC dari sistem file peserta. Jika subnet tumpang tindih, lalu lintas ke sistem file dapat terganggu.

Persyaratan dan pertimbangan subnet bersama

Saat membuat fsX untuk sistem file ONTAP ke subnet bersama, perhatikan hal berikut:

- Pemilik subnet VPC harus berbagi subnet dengan akun peserta sebelum akun tersebut dapat membuat FSx untuk sistem file ONTAP di dalamnya.
- Anda tidak dapat meluncurkan sumber daya menggunakan grup keamanan default untuk VPC karena milik pemilik. Selain itu, akun peserta tidak dapat meluncurkan sumber daya menggunakan grup keamanan yang dimiliki oleh peserta lain atau pemilik.
- Dalam subnet bersama, peserta dan pemilik secara terpisah mengontrol grup keamanan dalam setiap akun masing-masing. Akun pemilik dapat melihat grup keamanan yang dibuat oleh peserta, tetapi tidak dapat melakukan tindakan apa pun pada mereka. Jika akun pemilik ingin menghapus atau memodifikasi grup keamanan ini, peserta yang membuat grup keamanan harus mengambil tindakan.
- Akun peserta dapat melihat, membuat, memodifikasi, dan menghapus sistem file Single-AZ dan sumber daya terkait mereka dalam subnet yang telah dibagikan oleh akun pemilik dengan mereka.
- Akun peserta dapat membuat, melihat, memodifikasi, dan menghapus sistem file multi-AZ dan sumber daya terkait mereka dalam subnet yang telah dibagikan oleh akun pemilik dengan mereka. Selain itu, akun pemilik juga harus memberikan izin layanan Amazon FSx untuk mengubah tabel rute di subnet bersama atas nama akun peserta. Untuk informasi selengkapnya, lihat Mengelola dukungan VPC bersama untuk sistem file multi-AZ
- Pemilik VPC bersama tidak dapat melihat, memodifikasi, atau menghapus sumber daya yang dibuat peserta di subnet bersama. Ini merupakan tambahan dari sumber daya VPC yang setiap akun memiliki akses berbeda. Untuk informasi selengkapnya, lihat Tanggung jawab dan izin untuk pemilik dan peserta di Panduan Pengguna Amazon VPC.

Untuk informasi selengkapnya, lihat Berbagi VPC Anda dengan akun lain di Panduan Pengguna Amazon VPC.

Saat berbagi subnet VPC

Saat membagikan subnet Anda dengan akun peserta yang akan membuat fsX untuk sistem file ONTAP di subnet bersama, Anda perlu melakukan hal berikut:

- Pemilik VPC perlu menggunakannya AWS Resource Access Manager untuk berbagi VPC dan subnet dengan aman dengan lainnya. Akun AWS Untuk informasi selengkapnya, lihat Berbagi AWS sumber daya Anda di Panduan AWS Resource Access Manager Pengguna.
- Pemilik VPC perlu berbagi satu atau lebih VPC dengan akun peserta. Untuk informasi selengkapnya, lihat Berbagi VPC Anda dengan akun lain di Panduan Pengguna Amazon Virtual Private Cloud.
- Agar akun peserta dapat membuat FSx untuk sistem file Multi-AZ ONTAP, pemilik VPC juga harus memberikan izin layanan Amazon FSx untuk membuat dan memodifikasi tabel rute di subnet bersama atas nama akun peserta. Ini karena FSx untuk sistem file Multi-AZ ONTAP menggunakan alamat IP mengambang sehingga klien yang terhubung dapat dengan mulus bertransisi antara server file pilihan dan siaga selama acara failover. Ketika peristiwa failover terjadi, Amazon FSx memperbarui semua rute di semua tabel rute yang terkait dengan sistem file untuk menunjuk ke server file yang sedang aktif.

Mengelola dukungan VPC bersama untuk sistem file multi-AZ

Akun pemilik dapat mengelola apakah akun peserta dapat membuat Multi-AZ FSx untuk sistem file ONTAP di subnet VPC yang telah dibagikan pemilik dengan peserta menggunakan,, dan API AWS CLI, seperti AWS Management Console yang dijelaskan di bagian berikut.

Untuk mengelola berbagi VPC untuk sistem file Multi-AZ (konsol)

Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.

1. Pada panel navigasi, silakan pilih Pengaturan.
2. Temukan pengaturan VPC bersama Multi-AZ di halaman Pengaturan.

    - Untuk mengaktifkan berbagi VPC untuk sistem file multi-AZ di subnet VPC yang Anda bagikan, pilih Aktifkan pembaruan tabel rute dari akun peserta.
    - Untuk menonaktifkan berbagi VPC untuk sistem file multi-AZ di semua VPC yang Anda miliki, pilih Nonaktifkan pembaruan tabel rute dari akun peserta. Layar konfirmasi ditampilkan.

> **Important**
>
> Kami sangat menyarankan agar sistem file Multi-AZ yang dibuat oleh peserta di VPC bersama dihapus sebelum Anda menonaktifkan fitur ini. Setelah fitur dinonaktifkan, sistem file ini akan memasuki `MISCONFIGURED` status dan akan berisiko menjadi tidak tersedia.

3. Masuk **`confirm`** dan pilih Konfirmasi untuk menonaktifkan fitur.

Untuk mengelola berbagi VPC untuk sistem file Multi-AZ ()AWS CLI

1. Untuk melihat pengaturan saat ini untuk berbagi VPC multi-AZ, gunakan perintah CLI deskripsi-shared-vpc-konfigurasi, atau perintah API yang setara, yang ditunjukkan sebagai berikut: DescribeSharedVpcConfiguration

   ```
   $ aws fsx describe-shared-vpc-configuration
   ```

   Layanan menanggapi permintaan yang berhasil sebagai berikut:

   ```
   {
       "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
   }
   ```

2. Untuk mengelola konfigurasi VPC bersama Multi-AZ, gunakan perintah CLI update-shared-vpc-configuration, atau perintah API yang setara. UpdateSharedVpcConfiguration Contoh berikut memungkinkan berbagi VPC untuk sistem file Multi-AZ.

   ```
   $ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts true
   ```

   Layanan menanggapi permintaan yang berhasil sebagai berikut:

   ```
   {
       "EnableFsxRouteTableUpdatesFromParticipantAccounts": "true"
   }
   ```

3. Untuk menonaktifkan fitur, atur `EnableFsxRouteTableUpdatesFromParticipantAccounts` ke`false`, seperti yang ditunjukkan pada contoh berikut.

```
$ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts false
```

Layanan menanggapi permintaan yang berhasil sebagai berikut:

```
{
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
}
```

Memperbarui sistem file

Topik ini menjelaskan properti sistem file yang ada yang dapat Anda perbarui, dan menyediakan prosedur untuk melakukannya menggunakan konsol dan CLI.

Anda dapat memperbarui fsX berikut untuk properti sistem file ONTAP menggunakan konsol Amazon FSx, AWS CLI API Amazon FSx:

- Pencadangan harian otomatis. Mengaktifkan atau menonaktifkan pencadangan harian otomatis, memodifikasi jendela cadangan dan periode retensi cadangan. Untuk informasi selengkapnya tentang pencadangan, lihat Bekerja dengan backup harian otomatis.
- Jendela pemeliharaan mingguan. Menetapkan hari dalam seminggu dan waktu Amazon FSx melakukan pemeliharaan dan pembaruan sistem file. Untuk informasi selengkapnya tentang jendela pemeliharaan, lihatMengoptimalkan kinerja dengan jendela pemeliharaan Amazon FSx.
- Kata sandi administrasi sistem file. Mengubah kata sandi untuk `fsxadmin` pengguna sistem file. Anda dapat menggunakan `fsxadmin` pengguna untuk mengelola sistem file Anda menggunakan ONTAP CLI dan REST API. Untuk informasi selengkapnya tentang `fsxadmin` pengguna, lihatMengelola sistem file dengan ONTAP CLI.
- Tabel rute Amazon VPC. Dengan Multi-AZ FSx untuk sistem file ONTAP, titik akhir yang Anda gunakan untuk mengakses data melalui NFS atau SMB dan titik akhir manajemen untuk mengakses ONTAP CLI, API, dan BlueXP menggunakan alamat IP mengambang di tabel rute VPC Amazon yang Anda kaitkan dengan sistem file Anda. Anda dapat mengaitkan tabel rute baru yang Anda buat dengan sistem file multi-AZ yang ada—memungkinkan Anda mengonfigurasi klien

mana yang dapat mengakses data Anda bahkan saat jaringan Anda berkembang. Anda juga dapat memisahkan (menghapus) tabel rute yang ada dari sistem file Anda.

> **Note**
>
> Amazon FSx mengelola tabel rute VPC untuk sistem file multi-AZ menggunakan otentikasi berbasis tag. Tabel rute ini ditandai dengan`Key: AmazonFSx; Value: ManagedByAmazonFSx`. Saat membuat atau memperbarui FSx untuk sistem file Multi-AZ ONTAP menggunakan AWS CloudFormation kami sarankan Anda menambahkan tag secara manual. `Key: AmazonFSx; Value: ManagedByAmazonFSx`

Untuk memperbarui sistem file (konsol)

Prosedur berikut memberi Anda petunjuk tentang cara membuat pembaruan pada sistem file FSx untuk ONTAP yang ada menggunakan file. AWS Management Console

Untuk memperbarui backup harian otomatis

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Untuk menampilkan halaman detail sistem file, di panel navigasi kiri, pilih Sistem file, lalu pilih FSx untuk sistem file ONTAP yang ingin Anda perbarui.
3. Pilih tab Backup di panel kedua pada halaman.
4. Pilih Perbarui.
5. Ubah pengaturan cadangan harian otomatis untuk sistem file ini.
6. Pilih Simpan untuk menyimpan perubahan Anda.

Untuk memperbarui jendela pemeliharaan mingguan

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Untuk menampilkan halaman detail sistem file, di panel navigasi kiri, pilih Sistem file, lalu pilih FSx untuk sistem file ONTAP yang ingin Anda perbarui.
3. Pilih tab Administrasi di panel kedua pada halaman.
4. Di panel Pemeliharaan, pilih Perbarui.
5. Ubah kapan jendela pemeliharaan mingguan terjadi untuk sistem file ini.

6. Pilih Simpan untuk menyimpan perubahan Anda.

Untuk mengubah kata sandi administrasi sistem file

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Untuk menampilkan halaman detail sistem file, di panel navigasi kiri, pilih Sistem file, lalu pilih FSx untuk sistem file ONTAP yang ingin Anda perbarui.
3. Pilih tab Administrasi.
4. Di panel administrasi ONTAP, pilih Perbarui di bawah kata sandi administrator ONTAP.
5. Di kotak dialog Perbarui kredensi administrator ONTAP, masukkan kata sandi baru di bidang kata sandi administratif ONTAP.
6. Gunakan kolom Konfirmasi kata sandi untuk mengonfirmasi kata sandi.
7. Pilih Perbarui kredensi untuk menyimpan perubahan Anda.

> **Note**
>
> Jika Anda menerima kesalahan yang menyatakan bahwa kata sandi baru tidak memenuhi persyaratan kata sandi, Anda dapat menggunakan perintah `security login role config show`ONTAPCLI untuk melihat pengaturan persyaratan kata sandi pada sistem file. Untuk informasi selengkapnya, termasuk petunjuk tentang cara mengubah setelan kata sandi, lihatGagal memperbarui kata sandi `fsxadmin` akun.

Untuk memperbarui tabel rute VPC pada sistem file Multi-AZ

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Untuk menampilkan halaman detail sistem file, di panel navigasi kiri, pilih Sistem file, lalu pilih FSx untuk sistem file ONTAP yang ingin Anda perbarui.
3. Untuk Tindakan, pilih Kelola tabel rute. Opsi ini hanya tersedia untuk sistem file Multi-AZ.
4. Dalam kotak dialog Kelola tabel rute. lakukan salah satu hal berikut:

   - Untuk mengaitkan tabel rute VPC baru, pilih tabel rute dari daftar tarik-turun Tabel rute baru Associate, lalu pilih Associate.
   - Untuk memisahkan tabel rute VPC yang ada, pilih tabel rute dari panel Tabel rute saat ini, lalu pilih Pisahkan.

5. Pilih Tutup.

Untuk memperbarui sistem file (CLI)

Prosedur berikut menggambarkan cara membuat pembaruan ke FSx yang ada untuk sistem file ONTAP menggunakan file. AWS CLI

1. Untuk memperbarui konfigurasi FSx untuk sistem file ONTAP, gunakan perintah CLI update-file-system (atau operasi API UpdateFileSistem yang setara), seperti yang ditunjukkan pada contoh berikut.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --ontap-configuration
 AutomaticBackupRetentionDays=30,DailyAutomaticBackupStartTime=01:00, \
      WeeklyMaintenanceStartTime=1:01:30,AddRouteTableIds=rtb-0123abcd, \
      FsxAdminPassword=new-fsx-admin-password
```

2. Untuk menonaktifkan backup harian otomatis, atur `AutomaticBackupRetentionDays` properti ke 0.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --ontap-configuration AutomaticBackupRetentionDays=0
```

Menghapus sistem file

Anda dapat menghapus sistem file FSx untuk ONTAP menggunakan konsol Amazon FSx, AWS CLI API dan SDK Amazon FSx.

Untuk menghapus sistem file:

- Menggunakan konsol — Ikuti prosedur yang dijelaskan diLangkah 3: Bersihkan Sumber Daya .
- Menggunakan CLI atau API — Pertama hapus semua volume dan SVM pada sistem file Anda. Kemudian gunakan perintah CLI delete-file-system atau operasi API Sistem. DeleteFile

Melihat detail sistem file

Anda dapat melihat informasi konfigurasi terperinci untuk sistem file FSx untuk ONTAP menggunakan konsol Amazon FSx, API AWS CLI, dan SDK yang didukung. AWS

Untuk melihat informasi sistem file rinci:

- Menggunakan konsol — Pilih sistem file untuk melihat halaman detail sistem File. Panel Ringkasan menunjukkan ID sistem file, status siklus hidup, jenis penerapan, kapasitas penyimpanan SSD, kapasitas throughput, IOPS yang disediakan, Availability Zone, dan waktu pembuatan.

  Tab berikut menyediakan informasi konfigurasi terperinci dan pengeditan untuk properti yang dapat dimodifikasi:

  - Jaringan & keamanan
  - Pemantauan & kinerja - Menampilkan CloudWatch alarm yang telah Anda buat, serta metrik dan peringatan untuk kategori berikut:
    - Ringkasan — ringkasan tingkat tinggi dari metrik aktivitas sistem file
    - Kapasitas penyimpanan sistem file
    - Server file dan kinerja disk

    Untuk informasi selengkapnya, lihat Pemantauan CloudWatch dengan Amazon.
  - Administrasi - Menampilkan informasi administrasi sistem file berikut:
    - DNSNama dan IP alamat manajemen sistem file dan titik akhir antar-cluster.
    - Nama pengguna ONTAP administrator.
    - Opsi untuk memperbarui kata sandi ONTAP administrator.
  - Daftar SVM sistem file
  - Daftar volume sistem file
  - Pengaturan Backup — mengubah pengaturan backup harian otomatis sistem file.
  - Pembaruan - menunjukkan status pembaruan yang dimulai pengguna yang dibuat untuk konfigurasi sistem file.
  - Tag - lihat, edit, tambahkan, hapus tag Kunci: Pasangan nilai.
- Menggunakan CLI atau API - Gunakan perintah CLI deskripsi-file-sistem atau operasi API Sistem. DescribeFile

fsX untuk status sistem file ONTAP

Anda dapat melihat status sistem file Amazon FSx dengan menggunakan konsol Amazon FSx, AWS CLI perintah describe-file-systems, atau Sistem operasi API. DescribeFile

Status sistem file	Deskripsi
AVAILABLE	Sistem file telah berhasil dibuat dan tersedia untuk digunakan.
CREATING	Amazon FSx sedang membuat sistem file yang baru.
MENGHAPUS	Amazon FSx sedang menghapus sistem file yang ada.
SALAH KONFIGURASI	Sistem file berada dalam keadaan salah konfigurasi tetapi dapat dipulihkan.
GAGAL	1. Sistem file telah gagal dan Amazon FSx tidak dapat memulihkannya. 2. Saat membuat sistem file baru, Amazon FSx tidak dapat membuat sistem file yang baru.

Mengelola fsX untuk mesin virtual penyimpanan ONTAP

Di FSx untuk ONTAP, volume di-host di server file virtual yang disebut mesin virtual penyimpanan (SVM). SVM adalah server file terisolasi dengan kredensi administratifnya sendiri dan titik akhir untuk mengelola dan mengakses data. Saat Anda mengakses data di FSx untuk ONTAP, klien dan workstation Anda memasang volume, berbagi SMB, atau iSCSI LUN yang dihosting oleh SVM menggunakan titik akhir SVM (alamat IP).

Amazon FSx secara otomatis membuat SVM default pada sistem file Anda saat Anda membuat sistem file menggunakan. AWS Management Console Anda dapat membuat SVM tambahan di sistem file Anda kapan saja menggunakan konsol, AWS CLI, atau Amazon FSx API dan SDK. Anda tidak dapat membuat SVM menggunakan ONTAP CLI atau REST API.

Anda dapat menggabungkan SVM Anda ke Microsoft Active Directory untuk otentikasi dan otorisasi akses file. Untuk informasi selengkapnya, lihat Bekerja dengan Microsoft Active Directory di FSx untuk ONTAP.

Jumlah maksimum SVM per sistem file

Tabel berikut mencantumkan jumlah maksimum SVM yang dapat Anda buat untuk sistem file. Jumlah maksimum SVM tergantung pada jumlah kapasitas throughput yang disediakan dalam megabyte per detik (MBps).

Jenis deployment	Jumlah kapasitas throughput (MBps)	Jumlah maksimum SVM per sistem file
Single-AZ (peningkatan skala) dan Multi-AZ (peningkatan skala)	128	6
	256	6
	512	14
	1,024	14
	2,048	24
	4,096	24
Single-AZ (penskalaan)	Setiap	5

Topik

- Membuat mesin virtual penyimpanan
- Memperbarui mesin virtual penyimpanan
- Menghapus penyimpanan virtual machine (SVM)
- Melihat detail konfigurasi mesin virtual penyimpanan

Membuat mesin virtual penyimpanan

Anda dapat membuat FSx untuk ONTAP SVM menggunakan AWS Management Console,, AWS CLI dan API.

Jumlah maksimum SVM yang dapat Anda buat untuk sistem file tergantung pada jenis penyebaran sistem file Anda dan jumlah kapasitas throughput yang disediakan. Untuk informasi selengkapnya, lihat Jumlah maksimum SVM per sistem file.

Properti SVM

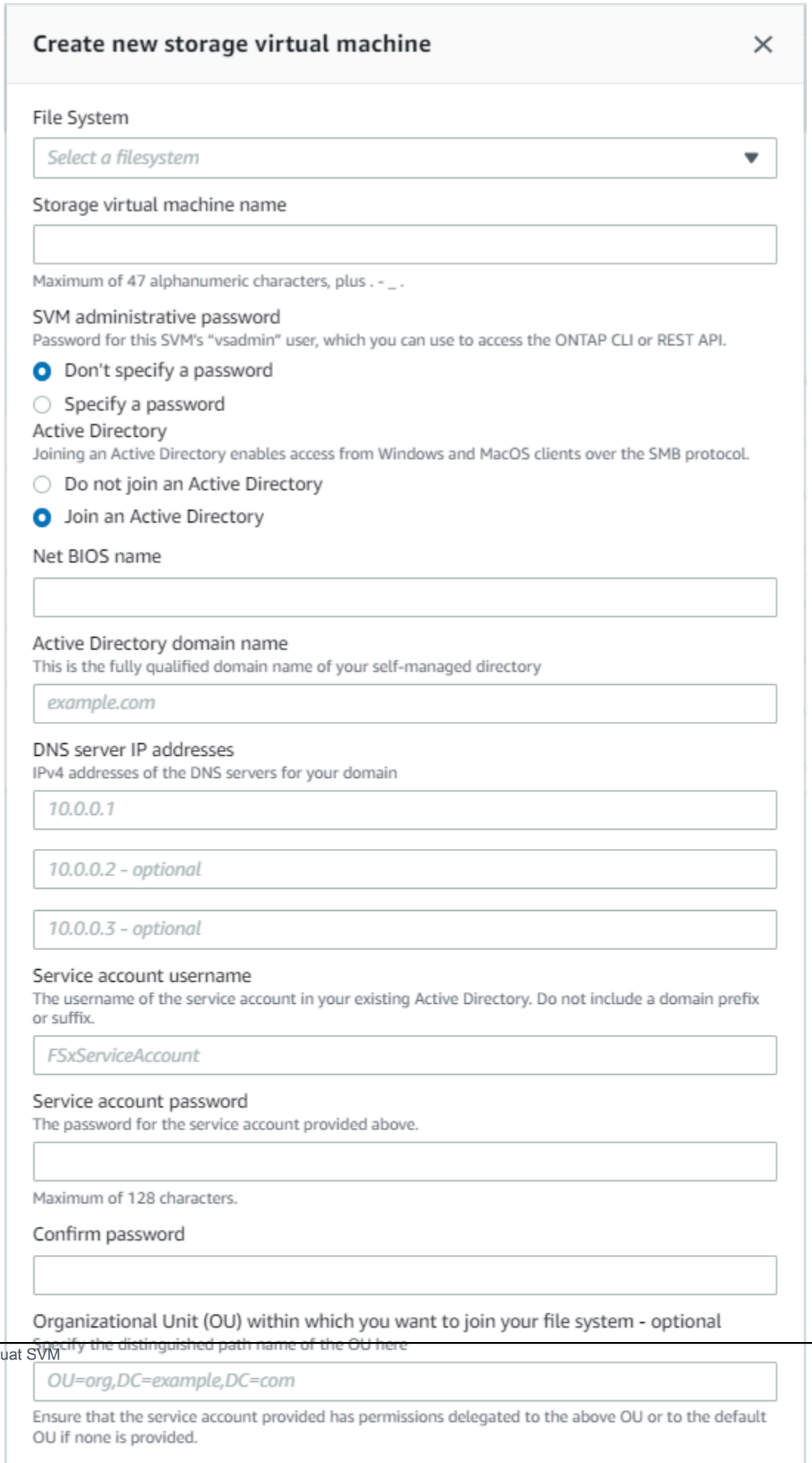
Saat membuat SVM, Anda menentukan properti berikut:

- FSx untuk sistem file ONTAP yang menjadi miliknya.
- Konfigurasi Microsoft Active Directory (AD) — Anda dapat secara opsional menggabungkan SVM Anda ke AD yang dikelola sendiri untuk otentikasi dan kontrol akses klien Windows dan macOS. Untuk informasi selengkapnya, lihat Bekerja dengan Microsoft Active Directory di FSx untuk ONTAP.
- Gaya keamanan volume root - Atur gaya keamanan volume root (Unix, NTFS, atau Mixed) agar selaras dengan jenis klien yang Anda gunakan untuk mengakses data Anda dalam SVM. Untuk informasi selengkapnya, lihat Gaya keamanan volume.
- Kata sandi administratif SVM — Anda dapat mengatur kata sandi untuk pengguna SVM secara opsional. `vsadmin` Untuk informasi selengkapnya, lihat Mengelola SVM dengan CLI ONTAP.

Untuk membuat penyimpanan mesin virtual (konsol)

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Di panel navigasi kiri, pilih Storage virtual machines.
3. Pilih Buat mesin virtual penyimpanan baru.

   Kotak dialog Create new storage virtual machine muncul.


Create new storage virtual machine
File System
Select a filesystem
Storage virtual machine name
Maximum of 47 alphanumeric characters, plus . - _ .
SVM administrative password
Password for this SVM's "vsadmin" user, which you can use to access the ONTAP CLI or REST API.
Don't specify a password
Specify a password
Active Directory
Joining an Active Directory enables access from Windows and MacOS clients over the SMB protocol.
Do not join an Active Directory
Join an Active Directory
Net BIOS name
Active Directory domain name
This is the fully qualified domain name of your self-managed directory
example.com
DNS server IP addresses
IPv4 addresses of the DNS servers for your domain
10.0.0.1
10.0.0.2 - optional
10.0.0.3 - optional
Service account username
The username of the service account in your existing Active Directory. Do not include a domain prefix or suffix.
FSxServiceAccount
Service account password
The password for the service account provided above.
Maximum of 128 characters.
Confirm password
Organizational Unit (OU) within which you want to join your file system - optional
Specify the distinguished path name of the OU here
OU=org,DC=example,DC=com
Ensure that the service account provided has permissions delegated to the above OU or to the default OU if none is provided.

4. Untuk sistem File, pilih sistem file untuk membuat mesin virtual penyimpanan.
5. Di bidang nama mesin virtual Penyimpanan, berikan nama untuk mesin virtual penyimpanan. Anda dapat menggunakan maksimal 47 karakter alfanumerik, ditambah karakter khusus garis bawah (_).
6. Untuk kata sandi administratif SVM, Anda dapat memilih Tentukan kata sandi dan berikan kata sandi untuk pengguna SVM ini. `vsadmin` Anda dapat menggunakan `vsadmin` pengguna untuk mengelola SVM menggunakan ONTAP CLI atau REST API. Untuk informasi selengkapnya tentang `vsadmin` pengguna, lihatMengelola SVM dengan CLI ONTAP.

   Jika Anda memilih Jangan tentukan kata sandi (default), Anda masih dapat menggunakan `fsxadmin` pengguna sistem file untuk mengelola sistem file Anda menggunakan ONTAP CLI atau REST API, tetapi Anda tidak dapat menggunakan pengguna SVM Anda untuk melakukan `vsadmin` hal yang sama.
7. Untuk Active Directory, Anda memiliki opsi berikut:

   - Jika Anda tidak bergabung dengan sistem file Anda ke Active Directory (AD), pilih Jangan bergabung dengan Active Directory.
   - Jika Anda bergabung dengan SVM Anda ke domain AD yang dikelola sendiri, pilih Bergabung dengan Direktori Aktif, dan berikan detail berikut untuk iklan Anda. Untuk informasi selengkapnya, lihat Prasyarat untuk bergabung dengan SVM ke Microsoft AD yang dikelola sendiri.
     - Nama NetBIOS dari objek komputer Active Directory yang akan dibuat untuk SVM Anda. Nama NetBIOS tidak boleh melebihi 15 karakter. Ini adalah nama SVM ini di Active Directory.
     - Nama domain yang sepenuhnya memenuhi syarat (FQDN) dari Direktori Aktif Anda. FQDN tidak dapat melebihi 255 karakter.
     - Alamat IP server DNS — Alamat IPv4 dari server DNS untuk domain Anda.
     - Nama pengguna akun layanan — Nama pengguna akun layanan di Direktori Aktif Anda yang ada. Jangan masukkan sebuah prefiks atau sufiks domain. Untuk`EXAMPLE\ADMIN`, gunakan`ADMIN`.
     - Kata sandi akun layanan — Kata sandi untuk akun layanan.
     - Konfirmasi kata sandi — Kata sandi untuk akun layanan.
     - (Opsional) Unit Organisasi (OU) - Nama jalur yang dibedakan dari unit organisasi tempat Anda ingin bergabung dengan sistem file Anda.

- Grup administrator sistem file yang didelegasikan — Nama grup di AD Anda yang dapat mengelola sistem file Anda.

  Jika Anda menggunakan AWS Managed Microsoft AD, Anda harus menentukan grup seperti Administrator FSx AWS Delegasi, Administrator Delegasi AWS , atau grup kustom dengan izin yang didelegasikan ke OU.

  Jika Anda bergabung dengan iklan yang dikelola sendiri, gunakan nama grup di iklan Anda. Grup defaultnya adalah`Domain Admins`.

8. Untuk gaya keamanan volume root SVM, pilih gaya keamanan untuk SVM tergantung pada jenis klien yang mengakses data Anda. Pilih Unix (Linux) jika Anda terutama mengakses data Anda menggunakan klien Linux; pilih NTFS jika Anda terutama mengakses data Anda menggunakan klien Windows. Untuk informasi selengkapnya, lihat Gaya keamanan volume.
9. Pilih Konfirmasi untuk membuat mesin virtual penyimpanan.

Anda dapat memantau kemajuan pembaruan pada halaman detail sistem file, di kolom Status panel mesin virtual Penyimpanan. Mesin virtual penyimpanan siap digunakan saat statusnya Dibuat.

Untuk membuat penyimpanan mesin virtual (CLI)

- Untuk membuat FSx untuk ONTAP storage virtual machine (SVM), gunakan perintah create-storage-virtual-machineCLI (atau operasi CreateStorageVirtualMachineAPI yang setara), seperti yang ditunjukkan pada contoh berikut.

```
aws fsx create-storage-virtual-machine \
    --file-system-id fs-0123456789abcdef0 \
    --name svm1 \
    --svm-admin-password password \
    --active-directory-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",FileSystemAd
 \
UserName="FSxService",Password="password", \
   DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

Setelah berhasil membuat mesin virtual penyimpanan, Amazon FSx mengembalikan deskripsinya dalam format JSON, seperti yang ditunjukkan pada contoh berikut.

```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef0123456789a",
    "StorageVirtualMachineId": "svm-abcdef0123456789a",
    "Subtype": "default",
    "Tags": [],
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
```

```
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
  }
}
```

Memperbarui mesin virtual penyimpanan

Anda dapat memperbarui properti konfigurasi mesin virtual penyimpanan (SVM) berikut menggunakan konsol Amazon FSx AWS CLI,, dan Amazon FSx API:

- Kata sandi akun administratif SVM.
- Konfigurasi SVM Active Directory (AD) — Anda dapat menggabungkan SVM ke AD, atau memodifikasi konfigurasi AD dari SVM yang sudah bergabung dengan AD. Untuk informasi selengkapnya, lihat Mengelola konfigurasi SVM Active Directory.

Untuk memperbarui kredensi akun administrator SVM (konsol)

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Pilih SVM yang akan diperbarui sebagai berikut:
   - Di panel navigasi kiri, pilih Sistem file, lalu pilih sistem file ONTAP yang ingin Anda perbarui SVM.
   - Pilih tab Storage Virtual Machines.

     —Atau—
   - Untuk menampilkan daftar semua SVM yang tersedia Akun AWS di Anda saat ini Wilayah AWS, perluas ONTAP dan pilih mesin virtual Penyimpanan.
3. Pilih mesin virtual penyimpanan yang ingin Anda perbarui.
4. Pilih Tindakan > Perbarui kata sandi administrator. Jendela Perbarui kredensi administratif SVM muncul.
5. Masukkan kata sandi baru untuk `vsadmin` pengguna, dan konfirmasikan.
6. Pilih Perbarui kredensi untuk menyimpan kata sandi baru.

Untuk memperbarui kredensi akun administrator SVM (CLI)

- Untuk memperbarui konfigurasi FSx untuk ONTAP SVM, gunakan perintah update-storage-virtual-machineCLI (atau operasi UpdateStorageVirtualMachineAPI yang setara), seperti yang ditunjukkan pada contoh berikut.

```
aws fsx update-storage-virtual-machine \
--storage-virtual-machine-id svm-abcdef01234567890 \
--svm-admin-password new-svm-password \
```

Setelah berhasil membuat mesin virtual penyimpanan, Amazon FSx mengembalikan deskripsinya dalam format JSON, seperti yang ditunjukkan pada contoh berikut.

```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
```

```
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef01234567890",
    "StorageVirtualMachineId": "svm-abcdef01234567890",
    "Subtype": "default",
    "Tags": [],
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
  }
}
```

Menghapus penyimpanan virtual machine (SVM)

Anda hanya dapat menghapus FSx untuk ONTAP SVM dengan menggunakan konsol Amazon FSx, API, dan. AWS CLI Sebelum Anda dapat menghapus SVM, Anda harus menghapus semua volume non-root yang dilampirkan ke SVM terlebih dahulu.

> **Important**
>
> Anda tidak dapat menghapus SVM dengan menggunakan NetApp ONTAP CLI atau API.

> **Note**
>
> Sebelum Anda menghapus mesin virtual penyimpanan, pastikan tidak ada aplikasi yang mengakses data di SVM, dan Anda telah menghapus semua volume non-root yang dilampirkan ke SVM.

Untuk menghapus penyimpanan mesin virtual (konsol)

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Pilih SVM yang ingin Anda hapus sebagai berikut:

   - Di panel navigasi kiri, pilih Sistem file, lalu pilih sistem file ONTAP yang ingin Anda hapus SVM.
   - Pilih tab Storage Virtual Machines.

   —Atau—

   - Untuk menampilkan daftar semua SVM yang tersedia, perluas ONTAP dan pilih mesin virtual Penyimpanan.

   Pilih SVM yang ingin Anda hapus dari daftar.
3. Di tab Volume, lihat daftar volume yang dilampirkan ke SVM. Jika ada volume non-root yang dilampirkan ke SVM, Anda harus menghapusnya sebelum Anda dapat menghapus SVM. Untuk informasi selengkapnya, lihat Menghapus volume.
4. Pilih Hapus penyimpanan virtual machine dari menu Actions.
5. Di kotak dialog hapus konfirmasi, pilih Hapus penyimpanan virtual machine.

Untuk menghapus penyimpanan mesin virtual (CLI)

- Untuk menghapus mesin virtual penyimpanan FSx ONTAP, gunakan perintah delete-storage-virtual-machineCLI (atau operasi DeleteStorageVirtualMachineAPI yang setara), seperti yang ditunjukkan pada contoh berikut.

```
aws fsx delete-storage-virtual-machine --storage-virtual-machine-id svm-
abcdef0123456789d
```

Melihat detail konfigurasi mesin virtual penyimpanan

Anda dapat melihat fsX untuk mesin virtual penyimpanan ONTAP yang saat ini ada di sistem file Anda menggunakan konsol Amazon FSx,, dan Amazon FSx AWS CLI API.

Untuk melihat mesin virtual penyimpanan pada sistem file Anda:

- Menggunakan konsol — Pilih sistem file untuk melihat halaman detail sistem File. Untuk mencantumkan semua mesin virtual penyimpanan pada sistem file, pilih tab Mesin virtual Penyimpanan, lalu pilih mesin virtual penyimpanan yang ingin Anda lihat.
- Menggunakan CLI atau API - Gunakan perintah describe-storage-virtual-machinesCLI atau operasi API. DescribeStorageVirtualMachines

  Respons sistem adalah daftar deskripsi lengkap dari semua SVM di akun Anda di dalamnya. Wilayah AWS

Mengelola FSx untuk volume ONTAP

Setiap mesin virtual penyimpanan (SVM) pada FSx untuk sistem file ONTAP dapat memiliki satu atau lebih volume. Volume adalah wadah data terisolasi untuk file, direktori, atau iSCSI logical unit of storage (LUNs). Volume tipis disediakan, artinya mereka mengkonsumsi kapasitas penyimpanan hanya untuk data yang tersimpan di dalamnya.

Anda dapat mengakses volume dari klien Linux, Windows, atau macOS melalui protokol Network File System (NFS), protokol Server Message Block (SMB), atau melalui protokol Internet Small Computer Systems Interface (iSCSI) dengan membuat iSCSI LUN (penyimpanan blok bersama). FSx untuk ONTAP juga mendukung akses multi-protokol (akses NFS dan SMB bersamaan) ke volume yang sama.

Anda dapat membuat volume dengan menggunakan AWS Management Console AWS CLI, Amazon FSx API, atau NetApp BlueXP. Anda juga dapat menggunakan sistem file atau titik akhir administratif SVM untuk membuat, memperbarui, dan menghapus volume dengan menggunakan NetApp ONTAP CLI atau REST API.

> **Note**
>
> Anda dapat membuat 500 volume per pasangan HA, hingga 1.000 volume di semua pasangan HA. FlexGroupvolume konstituen dihitung terhadap batas ini. Secara default, ada delapan volume konstituen per agregat, per. FlexGroup

Saat Anda membuat volume, Anda menentukan properti berikut:

- Gaya volume — Gaya volume dapat berupa FlexVol atauFlexGroup.
- Nama volume — Nama volume.
- Jenis volume - Jenis volume dapat berupa Read-Write (RW) atau Perlindungan data (DP). Volume DP adalah read-only dan digunakan sebagai tujuan dalam hubungan atau NetAppSnapMirror. SnapVault
- Ukuran volume — Ini adalah jumlah maksimum data yang dapat disimpan volume, terlepas dari tingkat penyimpanannya.
- Jalur persimpangan — Ini adalah lokasi di namespace SVM tempat volume dipasang.
- Efisiensi penyimpanan — Fitur efisiensi penyimpanan, termasuk pemadatan data, kompresi, dan deduplikasi memberikan penghematan penyimpanan tipikal sebesar 65% untuk beban kerja berbagi file tujuan umum.
- Gaya keamanan volume (Unix, NTFS, atau Mixed) - Menentukan jenis izin apa yang digunakan untuk akses data pada volume saat mengotorisasi pengguna.
- Tiering data — Kebijakan tiering mendefinisikan data mana yang disimpan dalam tingkat kumpulan kapasitas yang hemat biaya.
- Periode pendinginan kebijakan tingkat — Menentukan kapan data ditandai dingin dan dipindahkan ke penyimpanan kolam kapasitas.
- Kebijakan snapshot — Kebijakan snapshot menentukan cara sistem membuat snapshot untuk volume. Anda dapat memilih dari tiga kebijakan yang telah ditentukan sebelumnya atau menggunakan kebijakan kustom. yang telah Anda buat menggunakan ONTAP CLI atau REST API.
- Salin tag ke cadangan - Amazon FSx akan secara otomatis menyalin tag apa pun dari volume Anda ke cadangan menggunakan opsi ini. Anda dapat mengatur opsi ini menggunakan AWS CLI atau Amazon FSx API.

Topik

Gaya volume

FSx untuk ONTAP menawarkan dua gaya volume yang dapat Anda gunakan untuk tujuan yang berbeda. Anda dapat membuat salah satu FlexVol atau FlexGroup volume menggunakan konsol Amazon FSx, the AWS CLI, dan Amazon FSx API.

- FlexVolvolume menawarkan pengalaman paling sederhana untuk sistem file dengan satu pasangan ketersediaan tinggi (HA) dan merupakan gaya volume default untuk sistem file scale-up. Ukuran minimum FlexVol volume adalah 20 mebibytes (MiB), dan ukuran maksimum adalah 314.572.800 MiB.
- FlexGroupvolume terdiri dari beberapa FlexVol volume konstituen, yang memungkinkannya memberikan kinerja dan skalabilitas penyimpanan yang lebih tinggi daripada FlexVol volume untuk sistem file dengan beberapa pasangan HA. FlexGroupvolume adalah gaya volume default untuk sistem file scale-out. Ukuran minimum FlexGroup volume adalah 100 gibibytes (GiB) per konstituen, dan ukuran maksimum adalah 20 pebibytes (PiB).

Anda dapat mengonversi volume dengan FlexVol gaya ke FlexGroup gaya dengan ONTAP CLI, yang menciptakan a FlexGroup dengan satu konstituen. Namun, kami menyarankan Anda AWS DataSync untuk memindahkan data antara FlexVol volume dan FlexGroup volume baru untuk memastikan bahwa data didistribusikan secara merata di seluruh FlexGroup's konstituen. Untuk informasi selengkapnya, lihat FlexGroupkonstituen.

> **Note**
>
> Jika Anda ingin menggunakan ONTAP CLI untuk mengonversi FlexVol volume menjadi FlexGroup volume, pastikan Anda menghapus cadangan FlexVol volume sebelum mengonversinya. ONTAPtidak secara otomatis menyeimbangkan kembali data sebagai bagian dari konversi, sehingga data mungkin tidak seimbang di seluruh konstituen. FlexGroup

FlexGroupkonstituen

FlexGroupVolume terdiri dari konstituen, yaitu FlexVol volume. Secara default, FSx untuk ONTAP menetapkan delapan konstituen ke volume per pasangan HA. FlexGroup

Ketika Anda membuat FlexGroup volume Anda, ukurannya dibagi rata di antara konstituennya. Misalnya, jika Anda membuat FlexGroup volume 800 gigabyte (GB) dengan delapan konstituen, masing-masing konstituen berukuran 100 GB. FlexGroupVolume dapat berukuran antara 100 GB dan

20 PiB, tetapi ukuran totalnya tergantung pada ukuran konstituen. Setiap konstituen memiliki ukuran minimum 100 GB dan ukuran maksimum 300 TiB. Misalnya, FlexGroup volume dengan delapan konstituen memiliki ukuran minimum 800 GB dan ukuran maksimum 20 PiB.

ONTAP mendistribusikan data pada tingkat file di seluruh konstituen. Anda dapat menyimpan hingga dua miliar file di setiap konstituen pada FlexGroup volume Anda.

Saat Anda memperbarui ukuran FlexGroup volume Anda, ukuran baru didistribusikan secara merata di antara konstituen yang ada.

Anda juga dapat menambahkan lebih banyak konstituen ke FlexGroup volume Anda menggunakan ONTAP CLI atau REST API. Namun, kami menyarankan Anda hanya melakukannya jika Anda membutuhkan kapasitas penyimpanan tambahan dan semua konstituen Anda sudah pada ukuran maksimumnya (300 TiB per konstituen). Menambahkan konstituen dapat menyebabkan ketidakseimbangan data dan I/O di seluruh konstituen. Sampai konstituennya seimbang, mungkin saja throughput penulisan mungkin 5-10% lebih rendah dari volume seimbangFlexGroup. Ketika data baru ditulis ke FlexGroup volume, ONTAP memprioritaskan mendistribusikannya di antara konstituen baru sampai konstituen seimbang. Jika Anda menambahkan konstituen baru, kami sarankan memilih nomor genap dan tidak melebihi delapan per agregat.

> **Note**
>
> Jika Anda menambahkan konstituen baru, snapshot Anda yang ada menjadi snapshot sebagian; oleh karena itu, snapshot tersebut tidak dapat digunakan untuk mengembalikan FlexGroup volume Anda sepenuhnya ke status sebelumnya. Snapshot sebelumnya tidak dapat menawarkan point-in-time gambar lengkap FlexGroup volume Anda karena konstituen baru belum ada. Namun, sebagian snapshot dapat digunakan untuk memulihkan file dan direktori individual, untuk membuat volume baru, atau untuk mereplikasi dengan. SnapMirror

Tipe volume

FSx untuk ONTAP menawarkan dua jenis volume yang dapat Anda buat menggunakan konsol Amazon FSx, API, AWS CLI dan Amazon fsX.

- Volume baca-tulis (RW) digunakan dalam banyak kasus. Seperti namanya, mereka dapat dibaca.
- Volume perlindungan data (DP) adalah volume hanya-baca yang Anda gunakan sebagai tujuan suatu atau NetApp SnapMirror hubungan. SnapVault Anda harus menggunakan volume DP saat ingin memigrasi atau melindungi data satu volume.

FlexVoldan FlexGroup volume dapat berupa RW atau DP.

> **Note**
>
> Anda tidak dapat memperbarui jenis volume setelah volume dibuat.

Gaya keamanan volume

FSx untuk ONTAP mendukung 3 gaya keamanan volume yang berbeda: Unix, NTFS, dan campuran. Setiap gaya keamanan memiliki efek yang berbeda pada bagaimana izin ditangani untuk data. Anda harus memahami efek yang berbeda untuk memastikan bahwa Anda memilih gaya keamanan yang sesuai untuk tujuan Anda.

Penting untuk dipahami bahwa gaya keamanan tidak menentukan jenis klien apa yang dapat atau tidak dapat mengakses data. Gaya keamanan hanya menentukan jenis izin FSx untuk ONTAP gunakan untuk mengontrol akses data dan jenis klien apa yang dapat memodifikasi izin ini.

Dua faktor yang Anda gunakan untuk menentukan gaya keamanan untuk volume adalah jenis administrator yang mengelola sistem file dan jenis pengguna atau layanan yang mengakses data pada volume.

Saat membuat volume di konsol Amazon FSx, CLI, dan API, gaya keamanan secara otomatis diatur ke gaya keamanan volume root. Anda dapat memodifikasi gaya keamanan volume menggunakan API AWS CLI atau. Anda dapat mengubah pengaturan ini setelah volume dibuat. Untuk informasi selengkapnya, lihat Memperbarui volume.

Saat Anda mengonfigurasi gaya keamanan pada volume, pertimbangkan kebutuhan lingkungan Anda untuk memastikan bahwa Anda memilih gaya keamanan terbaik untuk menghindari masalah dalam mengelola izin. Perlu diingat bahwa gaya keamanan tidak menentukan tipe klien mana yang dapat mengakses data. Gaya keamanan menentukan izin yang digunakan untuk memungkinkan akses data dan jenis klien yang dapat mengubah izin tersebut. Berikut ini adalah pertimbangan yang dapat membantu Anda memutuskan gaya keamanan mana yang akan dipilih untuk volume:

- Unix (Linux) — Pilih gaya keamanan ini jika sistem file dikelola oleh administrator Unix, mayoritas pengguna adalah klien NFS, dan aplikasi yang mengakses data menggunakan pengguna Unix sebagai akun layanan. Hanya klien Linux yang dapat memodifikasi izin dengan gaya keamanan Unix, dan jenis izin yang digunakan pada file dan direktori adalah mode-bit atau NFS v4.x ACL.

- NTFS — Pilih gaya keamanan ini jika sistem file dikelola oleh administrator Windows, mayoritas pengguna adalah klien SMB, dan aplikasi yang mengakses data menggunakan pengguna Windows sebagai akun layanan. Jika ada akses Windows yang diperlukan untuk volume, kami sarankan Anda menggunakan gaya keamanan NTFS. Hanya klien Windows yang dapat memodifikasi izin dengan gaya keamanan NTFS, dan jenis izin yang digunakan pada file dan direktori adalah NTFS ACL.
- Campuran - Ini adalah pengaturan lanjutan. Untuk informasi selengkapnya, lihat topik Apa gaya keamanan dan efeknya di Pusat NetApp Dokumentasi.

Membuat volume

Anda dapat membuat FSx untuk ONTAP FlexVol atau FlexGroup volume menggunakan konsol Amazon FSx, API, dan Amazon fsX, AWS CLI selain antarmuka baris NetApp perintah ONTAP (CLI) dan REST API.

Untuk membuat FlexVol volume (konsol)

> **Note**
>
> Gaya keamanan volume secara otomatis diatur ke gaya keamanan volume root.

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Di panel navigasi kiri, pilih Volume.
3. Pilih Buat volume.
4. Untuk jenis sistem File, pilih Amazon FSx untuk NetApp ONTAP.
5. Di bagian Detail sistem berkas, berikan informasi berikut:
   - Untuk sistem File, pilih sistem file untuk membuat volume aktif.
   - Untuk mesin virtual Storage, pilih storage virtual machine (SVM) untuk membuat volume aktif.
6. Di bagian Gaya volume, pilih FlexVol.
7. Di bagian Detail volume, berikan informasi berikut:
   - Di bidang Nama volume, berikan nama untuk volume. Anda dapat menggunakan hingga 203 karakter alfanumerik atau garis bawah (_).

- Untuk ukuran Volume, masukkan bilangan bulat apa pun dalam kisaran 20—314572800 untuk menentukan ukuran dalam mebibytes (MiB).
- Untuk tipe Volume, pilih Read-Write (RW) untuk membuat volume yang dapat dibaca dan ditulis atau Perlindungan Data (DP) untuk membuat volume yang hanya-baca dan dapat digunakan sebagai tujuan hubungan atau. NetApp SnapMirror SnapVault Untuk informasi selengkapnya, lihat Tipe volume.
- Untuk jalur Junction, masukkan lokasi di dalam sistem file untuk me-mount volume. Nama harus memiliki garis miring ke depan, misalnya `/vol3`.
- Untuk efisiensi Penyimpanan, pilih Diaktifkan untuk mengaktifkan fitur efisiensi penyimpanan ONTAP (deduplikasi, kompresi, dan pemadatan). Untuk informasi selengkapnya, lihat fsX untuk efisiensi penyimpanan ONTAP.
- Untuk gaya keamanan Volume, pilih antara Unix (Linux), NTFS, dan Mixed untuk volume. Untuk informasi selengkapnya, lihat Gaya keamanan volume.
- Untuk kebijakan Snapshot, pilih kebijakan snapshot untuk volume. Untuk informasi selengkapnya tentang kebijakan snapshot, lihatKebijakan snapshot.

  Jika Anda memilih Kebijakan khusus, Anda harus menentukan nama kebijakan di bidang kebijakan khusus. Kebijakan kustom harus sudah ada di SVM atau di sistem file. Anda dapat membuat kebijakan snapshot khusus dengan ONTAP CLI atau REST API. Untuk informasi selengkapnya, lihat Membuat Kebijakan Snapshot di Dokumentasi Produk NetApp ONTAP.

8. Di bagian Storage tiering, berikan informasi berikut:

   - Untuk kebijakan tingkatan kumpulan Kapasitas, pilih kebijakan tiering kumpulan penyimpanan untuk volume, yang dapat berupa Otomatis (default), Hanya Snapshot, Semua, atau Tidak Ada. Untuk informasi selengkapnya, lihat Kebijakan tingkatan volume.
   - Jika Anda memilih Auto atau Snapshot Only, Anda dapat mengatur periode pendinginan kebijakan Tiering untuk menentukan jumlah hari sebelum data yang belum diakses ditandai dingin dan dipindahkan ke penyimpanan kolam kapasitas. Anda dapat memberikan nilai antara 2 dan 183 hari. Pengaturan default adalah 31 hari.

9. Di bagian Lanjutan, untuk SnapLockKonfigurasi, pilih antara Diaktifkan dan Dinonaktifkan. Untuk informasi selengkapnya tentang mengonfigurasi volume SnapLock Kepatuhan atau volume SnapLock Perusahaan, lihat Membuat Volume SnapLock Kepatuhan danMembuat volume SnapLock Enterprise. Untuk informasi selengkapnya tentang SnapLock, lihat Melindungi data Anda dengan SnapLock.
10. Pilih Konfirmasi untuk membuat volume.

Anda dapat memantau kemajuan pembaruan pada halaman detail sistem file, di kolom Status panel Volume. Volume siap digunakan saat statusnya Dibuat.

Untuk membuat FlexGroup volume (konsol)

> **Note**
>
> Anda hanya dapat membuat FlexGroup volume untuk sistem file scale-out menggunakan konsol Amazon FSx. Untuk membuat FlexVol volume untuk sistem file scale-out Anda, gunakan, AWS CLI Amazon FSx API, atau alat manajemen. NetApp

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Di panel navigasi kiri, pilih Volume.
3. Pilih Buat volume.
4. Untuk jenis sistem File, pilih Amazon FSx untuk NetApp ONTAP.
5. Di bagian Detail sistem berkas, berikan informasi berikut:
   - Untuk sistem File, pilih sistem file untuk membuat volume aktif.
   - Untuk mesin virtual Storage, pilih storage virtual machine (SVM) untuk membuat volume aktif.
6. Di bagian Gaya volume, pilih FlexGroup.
7. Di bagian Detail volume, berikan informasi berikut:
   - Di bidang Nama volume, berikan nama untuk volume. Anda dapat menggunakan hingga 203 karakter alfanumerik atau garis bawah (_).
   - Untuk ukuran Volume, masukkan bilangan bulat apa pun dalam kisaran 800 gibibyte (GiB) — 2.000 pebibytes (PiB).
   - Untuk tipe Volume, pilih Read-Write (RW) untuk membuat volume yang dapat dibaca dan ditulis atau Perlindungan Data (DP) untuk membuat volume yang hanya-baca dan dapat digunakan sebagai tujuan hubungan atau. NetApp SnapMirror SnapVault Untuk informasi selengkapnya, lihat Tipe volume.
   - Untuk jalur Junction, masukkan lokasi di dalam sistem file untuk me-mount volume. Nama harus memiliki garis miring ke depan, misalnya `/vol3`.
   - Untuk efisiensi Penyimpanan, pilih Diaktifkan untuk mengaktifkan fitur efisiensi penyimpanan ONTAP (deduplikasi, kompresi, dan pemadatan). Untuk informasi selengkapnya, lihat fsX untuk efisiensi penyimpanan ONTAP.

- Untuk gaya keamanan Volume, pilih antara Unix (Linux), NTFS, dan Mixed untuk volume. Untuk informasi selengkapnya, lihat Gaya keamanan volume.

> **Note**
>
> Gaya keamanan volume secara otomatis diatur ke gaya keamanan volume root.

- Untuk kebijakan Snapshot, pilih kebijakan snapshot untuk volume. Untuk informasi selengkapnya tentang kebijakan snapshot, lihatKebijakan snapshot.

  Jika Anda memilih Kebijakan khusus, Anda harus menentukan nama kebijakan di bidang kebijakan khusus. Kebijakan kustom harus sudah ada di SVM atau di sistem file. Anda dapat membuat kebijakan snapshot khusus dengan ONTAP CLI atau REST API. Untuk informasi selengkapnya, lihat Membuat Kebijakan Snapshot di Dokumentasi Produk NetApp ONTAP.

8. Di bagian Storage tiering, berikan informasi berikut:

   - Untuk kebijakan tingkatan kumpulan Kapasitas, pilih kebijakan tiering kumpulan penyimpanan untuk volume, yang dapat berupa Otomatis (default), Hanya Snapshot, Semua, atau Tidak Ada. Untuk informasi selengkapnya, lihat Kebijakan tingkatan volume.
   - Jika Anda memilih Auto atau Snapshot Only, Anda dapat mengatur periode pendinginan kebijakan Tiering untuk menentukan jumlah hari sebelum data yang belum diakses ditandai dingin dan dipindahkan ke penyimpanan kolam kapasitas. Anda dapat memberikan nilai antara 2-183 hari. Pengaturan default adalah 31 hari.

9. Di bagian Lanjutan, untuk SnapLockKonfigurasi, pilih antara Diaktifkan dan Dinonaktifkan. Untuk informasi selengkapnya tentang mengonfigurasi volume SnapLock Kepatuhan atau volume SnapLock Perusahaan, lihat Membuat Volume SnapLock Kepatuhan danMembuat volume SnapLock Enterprise. Untuk informasi selengkapnya tentang SnapLock, lihat Melindungi data Anda dengan SnapLock.
10. Pilih Konfirmasi untuk membuat volume.

Anda dapat memantau kemajuan pembaruan pada halaman detail sistem file, di kolom Status panel Volume. Volume siap digunakan saat statusnya Dibuat.

Untuk membuat volume (CLI)

- Untuk membuat FSx untuk volume ONTAP, gunakan perintah CLI create-volume (atau operasi CreateVolumeAPI yang setara), seperti yang ditunjukkan pada contoh berikut.

```
aws fsx create-volume \
    --volume-type ONTAP \
    --name vol1 \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/
vol1,SecurityStyle=NTFS, \
          SizeInMegabytes=1024,SnapshotPolicy=default, \
          StorageVirtualMachineId=svm-abcdef0123456789a,OntapVolumeType=RW, \
          StorageEfficiencyEnabled=true
```

Setelah berhasil membuat volume, Amazon FSx mengembalikan deskripsinya dalam format JSON, seperti yang ditunjukkan pada contoh berikut.

```
{
    "Volume": {
        "CreationTime": "2022-08-12T13:03:37.625000-04:00",
        "FileSystemId": "fs-abcdef0123456789c",
        "Lifecycle": "CREATING",
        "Name": "vol1",
        "OntapConfiguration": {
            "CopyTagsToBackups": true,
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "NTFS",
            "SizeInMegabytes": 1024,
            "SnapshotPolicy": "default",
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abcdef0123456789a",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "Name": "NONE"
            },
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-abcdef0123456789c/
fsvol-abcdef0123456789b",
        "VolumeId": "fsvol-abcdef0123456789b",
        "VolumeType": "ONTAP"


    }
```

```
}
```

Anda juga dapat membuat volume baru dengan mengembalikan cadangan volume ke volume baru. Untuk informasi selengkapnya, lihat Memulihkan backup ke volume baru.

Memperbarui volume

Anda dapat memperbarui konfigurasi FSx untuk volume ONTAP menggunakan konsol Amazon fsX, API, dan Amazon fsX, AWS CLI selain antarmuka baris NetApp perintah ONTAP (CLI) dan REST API. Anda dapat memodifikasi properti berikut dari fsX yang ada untuk volume ONTAP:

- Nama volume
- Jalur persimpangan
- Ukuran volume
- Efisiensi penyimpanan
- Kebijakan tingkatan kolam kapasitas
- Gaya keamanan volume
- Kebijakan snapshot
- Periode pendinginan kebijakan jenjang
- Salin tag ke cadangan (menggunakan API AWS CLI Amazon FSx dan)

Untuk informasi selengkapnya, lihat Mengelola FSx untuk volume ONTAP.

Untuk memperbarui konfigurasi volume (konsol)

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Arahkan ke sistem File dan pilih sistem file ONTAP yang ingin Anda perbarui volumenya.
3. Pilih tab Volume.
4. Pilih volume yang ingin Anda perbarui.
5. Untuk Tindakan, pilih Perbarui volume.

   Kotak dialog Perbarui volume ditampilkan dengan pengaturan volume saat ini.
6. Untuk jalur Junction, masukkan lokasi yang ada di dalam sistem file untuk me-mount volume. Nama harus memiliki garis miring ke depan, seperti `/vol5`.
7. Untuk ukuran Volume, Anda dapat menambah atau mengurangi ukuran volume dalam rentang yang ditentukan di konsol Amazon FSx. Untuk FlexVol volume, ukuran maksimum adalah 300

TiB. Untuk FlexGroup volume, ukuran maksimum adalah 300 TiB dikalikan dengan jumlah total volume konstituen yang Anda FlexGroup miliki, hingga maksimum 20 PiB.

8. Untuk efisiensi Penyimpanan, pilih Diaktifkan untuk mengaktifkan fitur efisiensi penyimpanan ONTAP (deduplikasi, kompresi, dan pemadatan), atau pilih Dinonaktifkan untuk menonaktifkannya.
9. Untuk kebijakan tingkatan kumpulan Kapasitas, pilih kebijakan tiering kumpulan penyimpanan baru untuk volume, yang dapat berupa Otomatis (default), khusus Snapshot, Semua, atau Tidak Ada. Untuk informasi selengkapnya tentang kebijakan tingkatan kumpulan kapasitas, lihatKebijakan tingkatan volume.
10. Untuk gaya keamanan Volume, pilih Unix (Linux), NTFS, atau Mixed. Gaya keamanan volume menentukan apakah preferensi diberikan ke NTFS atau UNIX ACL untuk akses multi-protokol. Mode MIXED tidak diperlukan untuk akses multi-protokol dan hanya direkomendasikan untuk pengguna tingkat lanjut.
11. Untuk kebijakan Snapshot, pilih kebijakan snapshot untuk volume. Untuk informasi selengkapnya tentang kebijakan snapshot, lihatKebijakan snapshot.

    Jika Anda memilih Kebijakan khusus, Anda harus menentukan nama kebijakan di bidang kebijakan khusus. Kebijakan kustom harus sudah ada di SVM atau di sistem file. Anda dapat membuat kebijakan snapshot khusus dengan ONTAP CLI atau REST API. Untuk informasi selengkapnya, lihat Membuat Kebijakan Snapshot di Dokumentasi Produk NetApp ONTAP.
12. Untuk periode pendinginan kebijakan Tiering, nilai yang berlaku adalah 2-183 hari. Periode pendinginan kebijakan tingkat volume menentukan jumlah hari sebelum data yang belum diakses ditandai dingin dan dipindahkan ke penyimpanan kolam kapasitas. Pengaturan ini hanya memengaruhi `Snapshot-only` kebijakan `Auto` dan kebijakan.
13. Pilih Perbarui untuk memperbarui volume.

Untuk memperbarui konfigurasi volume (CLI)

- Untuk memperbarui konfigurasi FSx untuk volume ONTAP, gunakan perintah CLI update-volume (atau operasi UpdateVolumeAPI yang setara), seperti yang ditunjukkan pada contoh berikut.

```
aws fsx update-volume \
    --volume-id fsvol-1234567890abcdefa \
    --name new_vol \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \
           SizeInMegabytes=2048,SnapshotPolicy=default-1weekly, \
           StorageEfficiencyEnabled=true, \
```

```
            TieringPolicy=all
```

Menghapus volume

Anda dapat menghapus FSx untuk volume ONTAP menggunakan konsol Amazon FSx, API, dan Amazon fsX, AWS CLI selain antarmuka baris NetApp perintah ONTAP (CLI) dan REST API.

> **Important**
>
> Anda hanya dapat menghapus volume menggunakan konsol Amazon FSx, API, atau CLI jika volume telah mengaktifkan cadangan Amazon FSx.

> **Important**
>
> Saat Anda menghapus volume dengan menggunakan konsol Amazon FSx, Anda memiliki opsi untuk mengambil cadangan akhir volume. Anda dapat membuat volume baru dari cadangan. Kami menyarankan Anda memilih untuk mengambil cadangan akhir sebagai praktik terbaik. Jika Anda merasa tidak membutuhkannya setelah jangka waktu tertentu, Anda dapat menghapus ini dan cadangan volume yang dibuat secara manual lainnya. Saat Anda menghapus volume dengan menggunakan perintah `delete-volume` CLI, Amazon FSx mengambil cadangan akhir secara default.

Sebelum Anda menghapus volume, pastikan tidak ada aplikasi yang mengakses data dalam volume yang ingin Anda hapus.

Untuk menghapus volume (konsol)

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Di panel navigasi kiri, pilih Sistem file, lalu pilih sistem file ONTAP yang ingin Anda hapus volumenya.
3. Pilih tab Volume.
4. Pilih volume yang ingin Anda hapus.
5. Untuk Tindakan, pilih Hapus volume.
6. Di kotak dialog konfirmasi, untuk Buat cadangan akhir, Anda memiliki dua opsi:

- Pilih Ya untuk mengambil cadangan akhir volume. Nama cadangan akhir ditampilkan.
- Pilih Tidak jika Anda tidak ingin cadangan akhir volume. Anda diminta untuk mengakui bahwa setelah volume dihapus, backup otomatis tidak lagi tersedia.

7. Konfirmasikan penghapusan volume dengan memasukkan hapus di bidang Konfirmasi hapus.
8. Pilih Hapus volume.

Untuk menghapus volume (CLI)

- Untuk menghapus FSx untuk volume ONTAP, gunakan perintah CLI hapus volume (atau operasi DeleteVolumeAPI yang setara), seperti yang ditunjukkan pada contoh berikut.

```
aws fsx delete-volume --volume-id fsvol-1234567890abcde
```

Melihat volume

Anda dapat melihat FSx untuk volume ONTAP yang saat ini ada di sistem file Anda menggunakan konsol Amazon FSx, AWS CLI API dan SDK Amazon FSx.

Untuk melihat volume pada sistem file Anda:

- Menggunakan konsol — Pilih sistem file untuk melihat halaman detail sistem File. Pilih tab Volume untuk mencantumkan semua volume pada sistem file, lalu pilih volume yang ingin Anda lihat.
- Menggunakan CLI atau API - Gunakan perintah CLI deskripsi-volume atau operasi API. DescribeVolumes

Membuat iSCSI LUN

Proses ini menjelaskan cara membuat iSCSI LUN di Amazon NetApp fsX untuk sistem file peningkatan skala ONTAP menggunakan perintah ONTAP CLI. NetApp lun create Untuk informasi selengkapnya, lihat lun createdi Pusat Dokumentasi NetApp ONTAP.

> **Note**
>
> Protokol iSCSI tidak didukung untuk sistem file scale-out.

Proses ini mengasumsikan Anda sudah memiliki volume yang dibuat pada sistem file Anda. Untuk informasi selengkapnya, lihat Membuat volume.

1. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen Amazon fsX NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Untuk informasi selengkapnya, lihat Mengelola sistem file dengan ONTAP CLI.

2. Buat LUN menggunakan perintah lun create NetApp CLI, menggantikan nilai-nilai berikut:

   - ***svm_name***- Nama mesin virtual penyimpanan (SVM) yang menyediakan target iSCSI. Tuan rumah menggunakan nilai ini untuk mencapai LUN.
   - ***vol_name***- Nama volume hosting LUN.
   - ***lun_name***- Nama yang ingin Anda tetapkan ke LUN.
   - ***size***- Ukuran, dalam byte, dari LUN. Ukuran maksimum LUN yang dapat Anda buat adalah 128 TB.

     > **Note**
     >
     > Kami menyarankan Anda menggunakan volume setidaknya 5% lebih besar dari ukuran LUN Anda. Margin ini menyisakan ruang untuk snapshot volume.

   - ***ostype***- Sistem operasi host, baik `windows_2008` atau`linux`. Gunakan `windows_2008` untuk semua versi Windows; ini memastikan LUN memiliki offset blok yang tepat untuk sistem operasi dan mengoptimalkan kinerja.

   > **Note**
   >
   > Sebaiknya aktifkan alokasi ruang pada LUN Anda. Dengan alokasi ruang diaktifkan, ONTAP dapat menginformasikan host Anda ketika LUN kehabisan kapasitas dan dapat merebut kembali ruang saat Anda menghapus data dari LUN.

   Untuk informasi selengkapnya, lihat `lun create`di dokumentasi CLI NetApp ONTAP.

```
> lun create -vserver svm_name -path /vol/vol_name/lun_name -size size -
ostype ostype -space-allocation enabled
```

```
Created a LUN of size 10g (10737418240)
```

3. Konfirmasikan LUN dibuat, online, dan dipetakan.

```
> lun show
```

Sistem merespons dengan output berikut:

```
Vserver   Path                            State   Mapped   Type         Size
--------- ------------------------------- ------- -------- ------------ --------
svm_name
          /vol/vol_name/lun_name          online  unmapped windows_2008 10GB
```

Langkah selanjutnya

Sekarang setelah Anda membuat iSCSI LUN, langkah selanjutnya dalam proses menggunakan iSCSI LUN sebagai penyimpanan blok adalah memetakan LUN ke file. `igroup` Untuk informasi selengkapnya, lihat Memasang iSCSI LUN ke klien Linux atau Memasang iSCSI LUN ke klien Windows.

Mengelola saham SMB

Untuk mengelola berbagi file SMB di sistem file Amazon FSx Anda, Anda dapat menggunakan GUI Folder Bersama Microsoft Windows. GUI Folder Bersama menyediakan lokasi pusat untuk mengelola semua folder bersama di mesin virtual penyimpanan (SVM) Anda. Prosedur berikut merinci cara membuat, memperbarui, dan menghapus berbagi file Anda.

> **Note**
>
> Anda juga dapat mengelola berbagi file SMB dengan menggunakan Manajer NetApp Sistem. Untuk informasi selengkapnya, lihat Menggunakan NetApp System Manager dengan BlueXP.

Untuk menghubungkan folder bersama ke sistem file Amazon FSx Anda

1. Luncurkan instans Amazon EC2 Anda dan hubungkan ke Direktori Aktif Microsoft yang tergabung dengan sistem file Amazon FSx Anda. Untuk melakukannya, pilih salah satu berikut dari Panduan Administrasi AWS Directory Service :

   - Bergabunglah dengan instans Windows EC2 dengan mulus
   - Bergabung dengan instance Windows secara manual
2. Connect ke instans Anda sebagai pengguna yang merupakan anggota dari grup administrator sistem file. Untuk informasi selengkapnya, lihat Menyambungkan ke Instans Windows Anda di Panduan Pengguna Amazon EC2.
3. Buka menu start dan jalankan fsmgmt.msc menggunakan Jalankan sebagai Administrator. Tindakan ini akan membuka alat GUI Folder Bersama.
4. Untuk Tindakan, pilih Connect ke komputer lain.
5. Untuk Komputer lain, masukkan nama DNS untuk mesin virtual penyimpanan Anda (SVM), misalnya. **`netbios_name.corp.example.com`**

   Untuk menemukan nama DNS SVM Anda di konsol Amazon FSx, pilih mesin virtual Storage, pilih SVM Anda, lalu gulir ke bawah ke Endpoints hingga Anda menemukan nama SMB DNS. Anda juga bisa mendapatkan nama DNS sebagai respons operasi DescribeStorageVirtualMachinesAPI.
6. Pilih OK. Entri untuk sistem file Amazon FSx Anda kemudian muncul dalam daftar untuk alat Folder Bersama.

Sekarang Folder Bersama terhubung ke sistem file Amazon FSx Anda, Anda dapat mengelola berbagi file Windows pada sistem file dengan tindakan berikut:

> **Note**
>
> Kami menyarankan Anda menemukan saham SMB Anda pada volume selain volume root Anda.

- Buat pembagian file baru — Di alat Folder Bersama, pilih Pembagian di sebelah kiri untuk melihat pembagian aktif untuk sistem file Amazon FSx Anda. Volume ditampilkan dipasang pada jalur yang dipilih selama pembuatan volume. Pilih Pembagian Baru dan selesaikan wizard Buat Folder Bersama.

Anda harus membuat folder lokal sebelum membuat pembagian file baru. Anda dapat melakukannya sebagai berikut:

- Menggunakan alat Folder Bersama: pilih Jelajahi saat menentukan jalur folder lokal, pilih Buat folder baru untuk membuat folder lokal.
- Menggunakan baris perintah:

```
New-Item -Type Directory -Path \\netbios_name.corp.example.com\C
$volume_path\MyNewFolder
```

- Mengubah pembagian file — Di alat Folder Bersama, buka menu konteks (klik kanan) untuk pembagian file yang ingin Anda ubah dalam panel kanan, lalu pilih Properti. Ubah properti dan pilih OKE.
- Menghapus pembagian file — Di alat Folder Bersama, buka menu konteks (klik kanan) untuk pembagian file yang ingin Anda hapus di panel kanan, lalu pilih Berhenti Berbagi.

> **Note**
>
> Menghapus berbagi file dari GUI hanya mungkin jika Anda terhubung ke fsmgmt.msc menggunakan nama DNS dari sistem file Amazon FSx. Jika Anda terhubung menggunakan alamat IP atau nama alias DNS dari sistem file, opsi Berhenti Berbagi tidak akan bekerja dan pembagian file tidak akan dihapus.

Mengaudit akses kunci

Amazon FSx for NetApp ONTAP men-support audit akses pengguna akhir ke file dan direktori di mesin virtual (SVM)

Topik

- Gambaran umum audit akses file
- Ikhtisar tugas untuk menyiapkan audit akses file

Gambaran umum audit akses file

Mengaudit akses file memungkinkan Anda merekam akses pengguna akhir atas file tunggal dan direktori tunggal berdasarkan kebijakan audit yang telah Anda tentukan. Audit akses file dapat

membantu Anda meningkatkan keamanan sistem dan mengurangi risiko akses tidak sah ke data sistem Anda. Audit akses file membantu organisasi Anda tetap mematuhi persyaratan perlindungan data, mengidentifikasi potensi ancaman sejak dini, dan mengurangi risiko pelanggaran data.

Di seluruh file dan direktori, Amazon FSx men-support pencatatan upaya yang berhasil (seperti pengguna dengan izin yang berhasil mengakses file), upaya yang gagal, atau keduanya. Anda juga dapat menonaktifkan audit akses file kapan saja.

Secara default, log peristiwa audit disimpan dalam format`EVTX` file, yang memungkinkan Anda melihatnya menggunakan Microsoft Event Viewer.

Peristiwa akses SMB yang dapat diaudit

Tabel berikut mencantumkan file SMB dan folder akses peristiwa dapat diaudit.

ID Acara (EVT/EVTX)	Peristiwa	Deskripsi	Kategori
560/4656	Buka Object/Buat Object	AKSES OBJEK: Objek (file atau direktori) terbuka	Akses file
563/4659	Buka Object dengan Intent to Delete	AKSES OBJEK: Pegangan ke objek (file atau direktori) diminta dengan Intent to Delete	Akses file
564/4660	Menghapus Objek	AKSES OBJEK: Hapus Object (file atau direktori). ONTAP menghasilkan acara ini ketika klien Windows mencoba untuk menghapus objek (file atau direktori)	Akses file
567/4663	Baca Objek/Tulis Objek/Dapatkan	AKSES OBJEK: Upaya akses objek	Akses file

ID Acara (EVT/EVTX)	Peristiwa	Deskripsi	Kategori
	Atribut Objek/Set Objek Atribut	(baca, tulis, dapatkan atribut, set atribut). **Note** Untuk acara ini, ONTAP hanya mengaudit operasi baca SMB pertama dan penulisan SMB pertama (sukses atau gagal) pada suatu objek. Ini mencegah ONTAP membuat entri log yang berlebiha n ketika satu klien membuka objek dan melakukan banyak operasi baca atau tulis berturut-turut ke objek yang sama.	

ID Acara (EVT/EVTX)	Peristiwa	Deskripsi	Kategori
N/4664	Tautan keras	AKSES OBJEK: Upaya dilakukan untuk membuat hard link	Akses file
N/A/N/A ONTAP ID Acara 9999	Ubah Nama Objek	OBJECT ACCESS: Object berganti nama. Ini adalah acara ONTAP. Saat ini tidak didukung oleh Windows sebagai acara tunggal.	Akses file
N/A/N/A ONTAP ID Acara 9998	Unlink Obyek	OBJEK ACCESS: Obyek unlinked. Ini adalah acara ONTAP. Saat ini tidak didukung oleh Windows sebagai acara tunggal.	Akses file

peristiwa akses NFS yang dapat diaudit

Peristiwa akses file dan folder NFS berikut dapat diaudit.

- MEMBACA
- BUKA
- TUTUP
- READDIR
- MENULIS
- SETATTR
- BUAT
- PRANALA

- OPENATTR
- REMOVE (HAPUS)
- GETATTR
- MEMVERIFIKASI
- NVERIFIKASI
- GANTI NAMA

Ikhtisar tugas untuk menyiapkan audit akses file

Menyiapkan FSx for ONTAP untuk audit akses file melibatkan tugas tingkat tinggi berikut ini:

1. Biasakan diri Anda dengan persyaratan dan pertimbangan audit akses file.
2. Buat konfigurasi audit pada SVM tertentu.
3. Aktifkan audit pada SVM itu.
4. Konfigurasikan kebijakan audit pada file dan direktori Anda.
5. Lihat log peristiwa audit setelah FSx untuk ONTAP memancarkannya.

Rincian tugas disediakan dalam prosedur berikut.

Ulangi tugas untuk SVM lain pada sistem file Anda yang ingin Anda aktifkan audit akses file

Persyaratan audit

Sebelum mengkonfigurasi dan mengaktifkan audit pada SVM, Anda harus mengetahui persyaratan dan pertimbangan berikut.

- NFS audit mendukung audit Access Control Entries (ACE) ditunjuk sebagai jenisu, yang menghasilkan entri log audit ketika akses dicoba pada objek. Untuk audit NFS, tidak ada pemetaan antara bit mode dan ACE audit. Saat mengonversi ACL ke bit mode, ACE audit dilewati. Saat mengonversi bit mode ke ACL, ACE audit tidak dihasilkan.
- Audit tergantung pada memiliki ruang yang tersedia dalam volume pementasan. (Volume pementasan adalah volume khusus yang dibuat oleh ONTAP untuk menyimpan file pementasan, yang merupakan file biner perantara pada node individu tempat catatan audit disimpan sebelum konversi ke format file EVTX atau XML.) Anda harus memastikan bahwa ada ruang yang cukup untuk volume pementasan dalam agregat yang berisi volume yang diaudit.

- Audit tergantung pada memiliki ruang yang tersedia dalam volume yang berisi direktori tempat log peristiwa audit yang dikonversi disimpan. Anda harus memastikan bahwa ada cukup ruang dalam volume yang digunakan untuk menyimpan log acara. Anda dapat menentukan jumlah log audit yang akan disimpan di direktori audit dengan menggunakan`-rotate-limit` parameter saat membuat konfigurasi audit, yang dapat membantu memastikan bahwa ada cukup ruang yang tersedia untuk log audit dalam volume.

Membuat konfigurasi audit pada SVM

Sebelum Anda dapat mulai mengaudit file dan direktori peristiwa, Anda harus membuat konfigurasi audit pada Storage Virtual Machine (SVM). Setelah membuat konfigurasi audit, Anda harus mengaktifkan pada SVM.

Sebelum Anda menggunakan`vserver audit create` perintah untuk membuat konfigurasi audit, pastikan Anda telah membuat direktori untuk digunakan sebagai tujuan untuk log, dan bahwa direktori tidak memiliki symlink. Anda menentukan direktori tujuan dengan`-destination` parameter.

Anda dapat membuat konfigurasi audit yang memutar log audit berdasarkan ukuran log atau jadwal, sebagai berikut:

- Untuk memutar log audit berdasarkan ukuran log, gunakan perintah ini:

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}] [-
rotate-limit integer] [-rotate-size {integer[KB|MB|GB|TB|PB]}]
```

  Contoh berikut membuat konfigurasi audit untuk SVM bernama`svm1` yang mengaudit operasi file dan logon CIFS (SMB) dan peristiwa logoff (default) menggunakan rotasi berbasis ukuran. Format log adalah`EVTX` (default), log disimpan dalam`/audit_log` direktori, dan Anda akan memiliki file log tunggal pada satu waktu (hingga 200MB dalam ukuran).

```
vserver audit create -vserver svm1 -destination /audit_log -rotate-size 200MB
```

- Untuk memutar log audit berdasarkan jadwal, gunakan perintah ini:

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}]
        [-rotate-limit integer] [-rotate-schedule-month chron_month]
        [-rotate-schedule-dayofweek chron_dayofweek] [-rotate-schedule-
day chron_dayofmonth]
        [-rotate-schedule-hour chron_hour] [-rotate-schedule-minute chron_minute]
```

`-rotate-schedule-minute`Parameter diperlukan jika Anda mengonfigurasi rotasi log audit berbasis waktu.

Contoh berikut membuat konfigurasi audit untuk SVM bernama`svm2` menggunakan rotasi berbasis waktu. Format log adalah`EVTX` (default) dan log audit diputar setiap bulan, pukul 12:30 pada semua hari dalam seminggu.

```
vserver audit create -vserver svm2 -destination /audit_log -rotate-size 200MB  -
rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour 12 -
rotate-schedule-minute 30
```

Anda dapat menggunakan`-format` parameter untuk menentukan apakah log audit dibuat dalam`EVTX` format yang dikonversi (default) atau dalam format`XML` file. `EVTX`Format ini memungkinkan Anda untuk melihat file log dengan Microsoft Event Viewer.

Secara default, kategori peristiwa yang akan diaudit adalah peristiwa akses file (baik SMB dan NFS), CIFS (SMB) logon dan peristiwa logoff, dan peristiwa perubahan kebijakan otorisasi. Anda dapat memiliki kontrol yang lebih besar atas peristiwa mana yang akan dicatat oleh`-events` parameter, yang memiliki format berikut:

```
-events {file-ops|cifs-logon-logoff|cap-staging|file-share|audit-policy-change|user-
account|authorization-policy-change|security-group}
```

Misalnya, menggunakan`-events file-share` memungkinkan audit peristiwa berbagi file.

Untuk informasi selengkapnya tentang`vserver audit create` perintah, lihat Membuat konfigurasi audit.

Mengaktifkan audit pada SVM

Setelah selesai menyiapkan konfigurasi audit, Anda harus mengaktifkan audit di SVM. Untuk melakukannya, gunakan perintah berikut:

```
vserver audit enable -vserver svm_name
```

Misalnya, gunakan perintah berikut untuk mengaktifkan audit pada SVM yang bernama`svm1`.

```
vserver audit enable -vserver svm1
```

Anda dapat menonaktifkan audit akses kapan saja. Misalnya, gunakan perintah berikut untuk menonaktifkan audit pada SVM bernamasvm4.

```
vserver audit disable -vserver svm4
```

Bila Anda menonaktifkan audit, konfigurasi audit tidak dihapus di SVM, yang berarti Anda dapat mengaktifkan kembali audit pada SVM tersebut kapan saja.

Mengkonfigurasi kebijakan audit file dan folder

Anda perlu mengkonfigurasi kebijakan audit pada file dan folder yang ingin Anda audit untuk upaya akses pengguna. Anda dapat mengonfigurasi kebijakan audit untuk memantau upaya akses yang berhasil dan gagal.

Anda dapat mengkonfigurasi kebijakan audit SMB dan NFS. Kebijakan audit SMB dan NFS memiliki persyaratan konfigurasi yang berbeda dan kemampuan audit berdasarkan gaya keamanan volume.

Kebijakan audit pada file dan direktori gaya keamanan NTFS

Anda dapat mengonfigurasi kebijakan audit NTFS dengan menggunakan tab Keamanan Windows atau CLI ONTAP.

Untuk mengkonfigurasi kebijakan audit NTFS (tab Keamanan Windows)

Anda mengkonfigurasi kebijakan audit NTFS dengan menambahkan entri ke NTFS SACL yang terkait dengan deskriptor keamanan NTFS. Deskriptor keamanan kemudian diterapkan ke file dan direktori NTFS. Tugas-tugas ini secara otomatis ditangani oleh GUI Windows. Deskriptor keamanan dapat berisi daftar kontrol akses diskresioner (DACL) untuk menerapkan izin akses file dan folder, SACL untuk audit file dan folder, atau SACl dan DACL.

1. Dari menu Alat di Windows Explorer, pilih Peta drive jaringan.
2. Lengkapi kotak Map Network Drive:

    a. Pilih huruf Drive.
    b. Di kotak Folder, ketik nama server SMB (CIFS) yang berisi berbagi, memegang data yang ingin Anda audit dan nama berbagi.
    c. Pilih Selesai.

    Drive yang Anda pilih sudah terpasang dan siap dengan jendela Windows Explorer yang menampilkan file dan folder yang terdapat di dalam share.

3. Pilih file atau direktori yang ingin Anda aktifkan akses audit.
4. Klik kanan pada file atau direktori, lalu pilih Properti.
5. Pilih tab Security.
6. Klik Lanjutan.
7. Pilih tab Audit.
8. Lakukan tindakan yang diinginkan:

Jika Anda ingin...	Lakukan hal berikut
Menyiapkan audit untuk pengguna atau grup baru	1. Pilih Tambahkan. 2. Di kotak Masukkan nama objek yang akan dipilih, ketik nama pengguna atau grup yang ingin Anda tambahkan. 3. Pilih OKE.
Menghapus audit dari pengguna atau grup	1. Di kotak Masukkan nama objek yang akan dipilih, pilih pengguna atau grup yang ingin Anda hapus. 2. Pilih Hapus. 3. Pilih OKE. 4. Lewati sisa prosedur ini.
Mengubah audit untuk pengguna atau grup	1. Di kotak Masukkan nama objek untuk dipilih, pilih pengguna atau grup yang ingin Anda ubah. 2. Pilih Edit. 3. Pilih OKE.

Jika Anda menyiapkan audit pada pengguna atau grup atau mengubah audit pada pengguna atau grup yang ada, kotak Entri Audit untuk ***objek*** akan terbuka.

9. Di kotak Terapkan ke, pilih bagaimana Anda ingin menerapkan entri audit ini.

   Jika Anda menyiapkan audit pada satu file, kotak Terapkan ke tidak aktif, karena default ke objek ini saja.

10. Di kotak Akses, pilih apa yang ingin diaudit dan apakah Anda ingin mengaudit peristiwa yang berhasil, peristiwa kegagalan, atau keduanya.

- Untuk mengaudit acara yang berhasil, pilih kotak Sukses.
- Untuk mengaudit kejadian kegagalan, pilih kotak Kegagalan.

Pilih tindakan yang perlu Anda pantau untuk memenuhi persyaratan keamanan Anda. Untuk informasi lebih lanjut tentang peristiwa audit ini, lihat dokumentasi Windows. Anda dapat mengaudit peristiwa berikut:

- Kontrol penuh
- Melintasi folder/mengeksekusi file
- Daftar folder/baca data
- Baca atribut
- Baca atribut diperpanjang
- Buat file/tulis data
- Buat folder/tambahkan data
- Tulis atribut
- Tulis atribut diperpanjang
- Menghapus subfolder dan file
- Hapus
- Izin baca
- Mengubah izin
- Ambil kepemilikan

11. Jika Anda tidak ingin pengaturan audit menyebar ke file dan folder berikutnya dari wadah asli, pilih kotak Terapkan entri audit ini ke objek dan/atau kontainer dalam kotak hanya kontainer ini.
12. Pilih Apply (Terapkan).
13. Setelah Anda selesai menambahkan, menghapus, atau mengedit entri audit, pilih OK.

    Kotak Entri Audit untuk ***objek*** ditutup.
14. Di kotak Audit, pilih pengaturan warisan untuk folder ini. Pilih hanya tingkat minimal yang menyediakan peristiwa audit yang memenuhi persyaratan keamanan Anda.

    Anda dapat memilih salah satu dari yang berikut ini:

- Pilih Sertakan entri audit yang dapat diwariskan dari kotak induk objek ini.

- Pilih kotak Ganti semua entri audit warisan yang ada pada semua keturunan dengan entri audit yang dapat diwariskan dari objek ini.
- Pilih kedua kotak.
- Pilih tidak ada kotak.

Jika Anda menyetel SACL pada satu file, kotak Ganti semua entri audit warisan yang ada pada semua keturunan dengan entri audit yang dapat diwariskan dari objek ini tidak ada di kotak Audit.

15. Pilih OKE.

Untuk mengkonfigurasi kebijakan audit NTFS (ONTAP CLI)

Dengan menggunakan ONTAP CLI, Anda dapat mengkonfigurasi kebijakan audit NTFS tanpa perlu terhubung ke data menggunakan berbagi SMB pada klien Windows.

- Anda dapat mengkonfigurasi kebijakan audit NTFS dengan menggunakan keluarga perintah direktori file keamanan vserver.

Misalnya, perintah berikut menerapkan kebijakan keamanan bernama`p1` SVM bernama`vs0`.

```
vserver security file-directory apply -vserver vs0 -policy-name p1
```

Kebijakan audit pada file dan direktori gaya keamanan UNIX

Anda mengkonfigurasi audit untuk file dan direktori gaya keamanan UNIX dengan menambahkan ACE audit (ekspresi kontrol akses) ke NFS v4.x ACL (daftar kontrol akses). Ini memungkinkan Anda untuk memantau acara akses file dan direktori NFS tertentu untuk tujuan keamanan.

> **Note**
>
> Untuk NFS v4.x, ACE diskresioner dan sistem disimpan dalam ACL yang sama. Oleh karena itu, Anda harus berhati-hati saat menambahkan ACE audit ke ACL yang ada untuk menghindari Timpa dan kehilangan ACL yang ada. Urutan di mana Anda menambahkan ACE audit ke ACL yang ada tidak masalah.

Untuk mengkonfigurasi kebijakan audit UNIX

1. Ambil ACL yang ada untuk file atau direktori dengan menggunakan perintah`nfs4_getfacl` atau setara.
2. Tambahkan ACE audit yang diinginkan.
3. Terapkan ACL yang diperbarui ke file atau direktori dengan menggunakan perintah`nfs4_setfacl` atau setara.

   Contoh ini menggunakan`-a` opsi untuk memberikan pengguna (bernama`testuser`) izin baca ke file bernama`file1`.

   ```
   nfs4_setfacl -a "A::testuser@example.com:R" file1
   ```

Melihat log event

Anda dapat melihat log peristiwa audit yang disimpan dalam format`EVTX` atau`XML` file.

- `EVTX`format file - Anda dapat membuka log peristiwa`EVTX` audit yang dikonversi sebagai file yang disimpan menggunakan Microsoft Event Viewer.

  Ada dua pilihan yang dapat Anda gunakan saat melihat log peristiwa menggunakan Event Viewer:
  - Tampilan umum: Informasi yang umum untuk semua acara ditampilkan untuk catatan acara. Data khusus peristiwa untuk catatan peristiwa tidak ditampilkan. Anda dapat menggunakan tampilan terperinci untuk menampilkan data khusus acara.
  - Tampilan terperinci: Tampilan ramah dan tampilan XMLtersedia. Tampilan ramah dan tampilan XMLmenampilkan kedua informasi yang umum untuk semua peristiwa dan data khusus peristiwa untuk catatan peristiwa.
- `XML`format file - Anda dapat melihat dan memproses log peristiwa audit XMLpada aplikasi pihak ketiga yang mendukung format file XML-nya. Alat tampilan XMLdapat digunakan untuk melihat log audit asalkan Anda memiliki skema XMLdan informasi tentang definisi untuk bidang XML-nya.

Menskalakan kapasitas penyimpanan SSD dan IOPS yang disediakan

Bila Anda membutuhkan penyimpanan tambahan untuk bagian aktif kumpulan data Anda, Anda dapat meningkatkan kapasitas penyimpanan solid state drive (SSD) Amazon FSx Anda untuk sistem

file NetApp ONTAP. Anda dapat melakukannya dengan menggunakan konsol Amazon FSx, Amazon FSx API, atau (). AWS Command Line Interface AWS CLI

Anda juga dapat mengubah IOPS SSD yang disediakan untuk sistem file Anda, baik ketika Anda meningkatkan kapasitas penyimpanan SSD utama atau sebagai tindakan independen. Untuk informasi selengkapnya tentang penskalaan kapasitas penyimpanan SSD utama sistem file dan jumlah IOPS yang disediakan, lihat. Memperbarui penyimpanan SSD sistem file dan IOPS

Mengelola kapasitas throughput

FSx untuk ONTAP mengonfigurasi kapasitas throughput saat Anda membuat sistem file. Anda dapat memodifikasi kapasitas throughput sistem file scale-up kapan saja, tetapi Anda tidak dapat mengubah kapasitas throughput sistem file scale-out Anda. Perlu diingat bahwa sistem file Anda memerlukan konfigurasi khusus untuk mencapai jumlah maksimum kapasitas throughput. Misalnya, untuk menyediakan kapasitas throughput 4 GBps untuk sistem file scale-up, sistem file Anda memerlukan konfigurasi dengan kapasitas penyimpanan SSD minimal 5.120 GiB dan 160.000 IOPS SSD. Untuk informasi selengkapnya, lihat Dampak kapasitas throughput terhadap performa.

Kapasitas throughput adalah salah satu faktor yang menentukan kecepatan di mana server file yang menghosting sistem file dapat melayani data file. Tingkat kapasitas throughput yang lebih tinggi datang dengan tingkat jaringan yang lebih tinggi, operasi I/O baca disk per detik (IOPS), dan kapasitas caching data pada server file. Untuk informasi selengkapnya, lihat Kinerja.

Saat Anda memodifikasi kapasitas throughput sistem file Anda, Amazon FSx mengalihkan server file yang memberi daya pada sistem file Anda. Sistem file Single-AZ dan Multi-AZ mengalami failover dan failback otomatis selama proses ini, yang biasanya membutuhkan waktu beberapa menit untuk menyelesaikannya. Proses failover dan failback transparan untuk klien NFS (Network File Sharing), SMB (Server Message Block), dan iSCSI (Internet Small Computer Systems Interface), memungkinkan beban kerja Anda terus berjalan tanpa gangguan atau intervensi manual. Anda ditagih untuk jumlah kapasitas throughput baru setelah tersedia untuk sistem file Anda.

> **Note**
>
> Untuk memastikan integritas data selama aktivitas pemeliharaan, FSx untuk ONTAP menutup semua kunci oportunistik dan menyelesaikan operasi penulisan yang tertunda ke volume penyimpanan dasar yang menghosting sistem file Anda sebelum pemeliharaan dimulai. Selama jendela pemeliharaan sistem file terjadwal, modifikasi sistem (seperti modifikasi kapasitas throughput Anda) mungkin tertunda. Pemeliharaan sistem dapat menyebabkan

perubahan ini mengantri hingga diproses. Untuk informasi selengkapnya, lihat the section called “Jendela pemeliharaan”.

Topik

- Kapan harus mengubah kapasitas throughput
- Bagaimana throughput bersamaan dan permintaan penskalaan penyimpanan ditangani
- Bagaimana cara mengubah kapasitas throughput
- Memantau perubahan kapasitas throughput pada konsol

Kapan harus mengubah kapasitas throughput

Amazon FSx terintegrasi dengan Amazon CloudWatch, yang membantu Anda memantau tingkat penggunaan throughput sistem file yang sedang berlangsung. Kinerja throughput dan IOPS yang dapat Anda dorong melalui sistem file tergantung pada karakteristik beban kerja spesifik Anda, selain kapasitas throughput sistem file Anda. Sebagai aturan, Anda harus menyediakan kapasitas throughput yang cukup untuk mendukung throughput baca beban kerja Anda ditambah dua kali throughput penulisan beban kerja Anda. Anda dapat menggunakan CloudWatch metrik untuk menentukan dimensi mana yang akan diubah untuk meningkatkan kinerja. Untuk informasi selengkapnya, lihat the section called “Cara menggunakan fsX untuk metrik ONTAP CloudWatch”.

Note

Anda tidak dapat mengubah kapasitas throughput untuk sistem file scale-out.

Bagaimana throughput bersamaan dan permintaan penskalaan penyimpanan ditangani

Anda dapat meminta pembaruan kapasitas throughput tepat sebelum kapasitas penyimpanan SSD dan alur kerja pembaruan IOPS yang disediakan dimulai atau saat sedang berlangsung. Urutan bagaimana Amazon FSx menangani dua permintaan adalah sebagai berikut:

- Jika Anda mengirimkan pembaruan SSD/IOPS dan pembaruan kapasitas throughput secara bersamaan, kedua permintaan diterima. Pembaruan SSD/IOPS diprioritaskan sebelum pembaruan kapasitas throughput.

- Jika Anda mengirimkan pembaruan kapasitas throughput saat pembaruan SSD/IOPS sedang berlangsung, permintaan pembaruan kapasitas throughput diterima dan diantrian terjadi setelah pembaruan SSD/IOPS. Pembaruan kapasitas throughput dimulai setelah SSD/IOPS diperbarui (nilai baru tersedia) dan selama langkah pengoptimalan. Ini biasanya memakan waktu kurang dari 10 menit.
- Jika Anda mengirimkan pembaruan SSD/IOPS saat pembaruan kapasitas throughput sedang berlangsung, permintaan pembaruan penyimpanan SSD/IOPS diterima dan diantri untuk memulai setelah pembaruan kapasitas throughput selesai (kapasitas throughput baru tersedia). Ini biasanya memakan waktu 20 menit.

Untuk informasi selengkapnya tentang penyimpanan SSD dan pembaruan IOPS yang disediakan, lihat. Mengelola kapasitas penyimpanan

Bagaimana cara mengubah kapasitas throughput

Anda dapat mengubah kapasitas throughput pada sistem file dengan menggunakan konsol Amazon FSx, AWS Command Line Interface (AWS CLI), atau API Amazon FSx.

Untuk mengubah kapasitas throughput sistem file (CLI)

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Arahkan ke sistem File, dan pilih sistem file ONTAP yang ingin Anda tingkatkan kapasitas throughputnya.
3. Untuk Tindakan, pilih Perbarui kapasitas throughput. Atau, pada panel Ringkasan, pilih Perbarui di samping Kapasitas throughput pada sistem file.
4. Pilih nilai baru untuk Kapasitas throughput dari daftar.

> **Note**
>
> Anda dapat mengubah kapasitas throughput untuk FSx apa pun untuk sistem file ONTAP. Namun, hanya sistem file yang dibuat pada atau setelah 9 Desember 2021 yang dapat mendukung kapasitas throughput 128 MB/s atau 256 MB/s.

5. Pilih Perbarui untuk memulai pembaruan kapasitas throughput.
6. Anda dapat memantau kemajuan pembaruan pada halaman detail sistem File, pada tab Pembaruan.

Anda dapat memantau perkembangan pembaruan dengan menggunakan konsol Amazon FSx, AWS CLI, dan API. Untuk informasi selengkapnya, lihat Memantau perubahan kapasitas throughput pada konsol.

Untuk mengubah kapasitas throughput sistem file (CLI)

Untuk memodifikasi kapasitas throughput sistem file, gunakan AWS CLI perintah update-file-system. Atur parameter berikut:

- `--file-system-id` untuk ID dari sistem file yang Anda perbarui.
- `ThroughputCapacity` untuk nilai yang diinginkan untuk memperbarui properti sistem file.

Anda dapat memantau perkembangan pembaruan dengan menggunakan konsol Amazon FSx, AWS CLI, dan API. Untuk informasi selengkapnya, lihat Memantau perubahan kapasitas throughput pada konsol.

Memantau perubahan kapasitas throughput pada konsol

Anda dapat memantau perkembangan peningkatan kapasitas throughput menggunakan konsol Amazon FSx, API, atau AWS CLI.

Memantau perubahan kapasitas throughput pada konsol

Pada tab Pembaruan di jendela Rincian sistem file, Anda dapat melihat 10 tindakan pembaruan terbaru untuk setiap jenis tindakan pembaruan.

Untuk melakukan tindakan pembaruan kapasitas throughput, Anda dapat melihat informasi berikut.

Jenis pembaruan

Jenis yang didukung adalah Kapasitas throughput, Kapasitas penyimpanan, dan Optimisasi penyimpanan.

Nilai target

Nilai yang diinginkan untuk mengubah kapasitas throughput pada sistem file.

Status

Status terkini dari pembaruan tersebut. Untuk pembaruan kapasitas throughput, nilai yang mungkin didapat adalah sebagai berikut:

- Tertunda – Amazon FSx telah menerima permintaan pembaruan, namun belum mulai memprosesnya.
- Dalam proses – Amazon FSx sedang memproses permintaan pembaruan.
- Selesai – Pembaruan kapasitas throughput berhasil diselesaikan.
- Gagal – Pembaruan kapasitas throughput gagal. Pilih tanda tanya (?) untuk melihat secara terperinci mengapa pembaruan throughput gagal.

Waktu permintaan

Waktu ketika Amazon FSx menerima permintaan pembaruan.

Memantau perubahan dengan AWS CLI dan API

Anda dapat melihat dan memantau permintaan modifikasi kapasitas throughput sistem file menggunakan perintah describe-file-systemsCLI dan tindakan API DescribeFileSystems. Daftar `AdministrativeActions` berisi 10 tindakan pembaruan terkini untuk setiap jenis tindakan administratif. Jika Anda mengubah kapasitas throughput sistem file, muncul sebuah tindakan administratif `FILE_SYSTEM_UPDATE`.

Contoh berikut menunjukkan kutipan tanggapan atas perintah CLI `describe-file-systems`. Sistem file memiliki kapasitas throughput 128 MB/s, dan kapasitas throughput target 256 MB/s.

```
.
.
.
    "ThroughputCapacity": 128,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "OntapConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

Saat Amazon FSx berhasil memproses tindakan, statusnya berubah menjadi. `COMPLETED` Kapasitas throughput yang baru kemudian tersedia untuk sistem file tersebut, dan tampak dalam properti `ThroughputCapacity`. Ini ditunjukkan dalam kutipan tanggapan atas perintah CLI describe-file-systems berikut.

```
.
.
.
    "ThroughputCapacity": 256,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "COMPLETED",
        "TargetFileSystemValues": {
          "OntapConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

Jika perubahan kapasitas throughput gagal, statusnya berubah menjadi `FAILED`, dan properti `FailureDetails` memberikan informasi tentang kegagalan tersebut.

Mengoptimalkan kinerja dengan jendela pemeliharaan Amazon FSx

Sebagai layanan yang dikelola sepenuhnya, FSx untuk ONTAP secara teratur melakukan pemeliharaan dan pembaruan ke sistem file Anda. Pemeliharaan ini tidak berdampak pada sebagian besar beban kerja. Untuk beban kerja yang sensitif terhadap kinerja, pada kesempatan langka Anda mungkin melihat dampak singkat (<60 detik) pada kinerja saat pemeliharaan terjadi; Amazon FSx memungkinkan Anda menggunakan jendela pemeliharaan untuk mengontrol kapan aktivitas pemeliharaan potensial tersebut terjadi.

Patching jarang terjadi, biasanya setiap beberapa minggu sekali. Untuk sistem file scale-up, patching biasanya hanya membutuhkan waktu 30 menit dari awal jendela pemeliharaan Anda. Untuk sistem file scale-out, patching membutuhkan waktu hingga 90 menit dari awal jendela pemeliharaan Anda. Selama beberapa menit ini, sistem file Anda secara otomatis gagal dan gagal kembali. Anda memilih

jendela pemeliharaan selama pembuatan sistem file. Jika Anda tidak memiliki preferensi waktu, maka waktu mulai 30 menit ditetapkan.

FSx untuk ONTAP memungkinkan Anda menyesuaikan jendela pemeliharaan sesuai kebutuhan untuk mengakomodasi beban kerja dan persyaratan operasional Anda. Anda dapat memindahkan jendela pemeliharaan sesering yang diperlukan, asalkan jendela pemeliharaan terjadi setidaknya sekali setiap 14 hari. Jika patch dilepaskan dan jendela pemeliharaan tidak terjadi dalam 14 hari, fsX untuk ONTAP akan melanjutkan pemeliharaan pada sistem file untuk memastikan keamanan dan keandalannya.

> **Note**
>
> Untuk memastikan integritas data selama aktivitas pemeliharaan, FSx untuk ONTAP menutup semua kunci oportunistik dan menyelesaikan operasi penulisan yang tertunda ke volume penyimpanan dasar yang menghosting sistem file Anda sebelum pemeliharaan dimulai.

Anda dapat menggunakan Amazon FSx Management Console AWS CLI, AWS API, atau salah satu AWS SDK untuk mengubah jendela pemeliharaan sistem file Anda.

Untuk mengubah jendela (konsol) pemeliharaan mingguan

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Pilih Sistem file di kolom navigasi sebelah kiri.
3. Pilih sistem file yang ingin Anda ubah jendela pemeliharaan mingguannya. Halaman detail sistem file Ringkasan muncul.
4. Pilih Administrasi untuk menampilkan panel Pengaturan administrasi sistem file.
5. Pilih Perbarui untuk menampilkan jendela Ubah waktu pemeliharaan.
6. Masukkan hari dan waktu baru yang Anda ingin jendela pemeliharaan mingguannya dimulai.
7. Pilih Simpan untuk menyimpan perubahan Anda. Waktu mulai pemeliharaan baru ditampilkan di panel Pengaturan administrasi sistem file.

Untuk mengubah jendela pemeliharaan mingguan menggunakan perintah update-file-systemCLI, lihat. Untuk memperbarui sistem file (CLI)

Memberi tanda sumber daya Amazon FSx Anda

Untuk membantu Anda mengelola sistem file dan sumber daya Amazon FSx lainnya, Anda dapat menetapkan metadata Anda sendiri ke setiap sumber daya dalam bentuk tanda. Dengan tanda, Anda dapat mengategorikan AWS sumber daya Anda dengan berbagai cara, misalnya, berdasarkan tujuan, pemilik, atau lingkungan. Kategorisasi ini berguna ketika Anda memiliki banyak sumber daya dengan jenis yang sama—Anda dapat dengan segera mengidentifikasi sumber daya tertentu berdasarkan tanda yang telah Anda tetapkan. Topik ini menjelaskan tanda dan menunjukkan kepada Anda cara membuatnya.

Topik

Dasar tanda

Tanda adalah label yang Anda tetapkan ke sumber daya AWS. Setiap tag terdiri dari dua bagian yang Anda tentukan:

- Sebuah kunci tag (misalnya, `CostCenter`, `Environment`, atau `Project`). Kunci tag peka huruf besar dan kecil.
- Nilai tag (misalnya, `111122223333` atau`Production`). Seperti kunci tanda, nilai tanda peka huruf besar dan kecil. Nilai tag bersifat opsional.

Anda dapat menggunakan tanda untuk mengategorikan AWS sumber daya Anda dengan berbagai cara, misalnya, berdasarkan tujuan, pemilik, atau lingkungan. Misalnya, Anda dapat menentukan serangkaian tanda untuk sistem file Amazon FSx akun Anda yang dapat membantu Anda melacak setiap pemilik dan tingkat tumpukan instans.

Sebaiknya Anda merancang seperangkat kunci tanda yang memenuhi kebutuhan Anda untuk setiap jenis sumber daya. Penggunaan seperangkat kunci tanda yang konsisten akan mempermudah Anda

dalam mengelola sumber daya Anda. Anda dapat mencari dan memfilter sumber daya berdasarkan tanda yang Anda tambahkan. Untuk informasi lebih lanjut tentang cara pelaksanaan strategi penandaan sumber daya yang efektif, lihat Memberi tag pada AWS sumber daya. Referensi Umum AWS

Beberapa perilaku penandaan yang perlu diingat:

- Tanda tidak memiliki makna semantik pada Amazon FSx dan diterjemahkan sebagai serangkaian karakter saja.
- Selain itu, tanda tidak dapat menetapkan secara otomatis ke sumber daya Anda.
- Anda dapat mengedit kunci dan nilai tanda, dan Anda dapat menghapus tanda dari sumber daya pada saat kapan pun.
- Anda dapat mengatur nilai tanda menjadi sebuah string kosong, tetapi Anda tidak dapat mengatur nilai tanda menjadi`null`.
- Jika Anda menambahkan tanda yang memiliki kunci yang sama dengan tanda yang telah ada pada sumber daya tersebut, nilai yang baru akan menimpa nilai yang lama.
- Jika Anda menghapus sumber daya, semua tanda untuk sumber daya tersebut juga dihapus.
- Jika Anda menggunakan Amazon FSx API, AWS Command Line Interface (AWS CLI), atau AWS SDK, Anda dapat melakukan hal berikut:
  - Anda dapat menggunakan tindakan `TagResource` API untuk menerapkan tanda ke sumber daya yang ada.
  - Untuk beberapa tindakan pembuatan sumber daya, Anda dapat menentukan tanda untuk sumber daya saat sumber daya diciptakan. Dengan menandai sumber daya pada saat pembuatan, Anda dapat menghilangkan kebutuhan untuk menjalankan skrip penandaan khusus setelah pembuatan sumber daya.

    Jika tanda tidak dapat diterapkan selama pembuatan sumber daya, Amazon FSx me-rollback proses penciptaan sumber daya. Perilaku ini membantu memastikan bahwa sumber daya diciptakan dengan tanda atau tidak dibuat sama sekali, dan tidak akan ada sumber daya yang dibiarkan tidak ditandai.

    > **Note**
    >
    > Izin tertentu AWS Identity and Access Management (IAM) diperlukan bagi pengguna untuk memberi tag pada sumber daya saat penciptaan. Untuk informasi selengkapnya,

lihat Memberikan izin untuk memberi tanda pada sumber daya saat sumber daya tersebut dibuat.

Menandai Sumber Daya Anda

Anda dapat memberi tag pada sumber daya Amazon FSx yang ada dalam akun Anda. Jika Anda menggunakan konsol Amazon FSx, Anda dapat menerapkan tanda ke sumber daya dengan menggunakan tab Tags pada layar sumber daya yang relevan. Ketika Anda membuat sumber daya, Anda dapat menerapkan kunci Nama dengan nilai, dan Anda dapat menerapkan tag pilihan Anda saat membuat sistem file baru. Namun, meskipun konsol mengorganisasi sumber daya sesuai dengan kunci Name, kunci ini tidak memiliki makna semantik pada layanan Amazon FSx.

Untuk mengimplementasikan kontrol terperinci atas pengguna dan grup yang dapat memberi tag pada sumber daya saat penciptaan, Anda dapat menerapkan izin tingkat sumber daya berbasis tag dalam kebijakan IAM Anda untuk tindakan Amazon FSx API yang mendukung penandaan saat pembuatan. Dengan menggunakan izin tersebut dalam kebijakan Anda, Anda mendapat manfaat berikut:

- Sumber daya Anda diamankan dari penciptaan.
- Karena tanda diterapkan segera ke sumber daya Anda, izin tingkat sumber daya berbasis tanda apa pun yang mengontrol penggunaan sumber daya akan efektif segera.
- Sumber daya Anda dapat dilacak dan dilaporkan dengan lebih akurat.
- Anda dapat menerapkan penggunaan penandaan pada sumber daya baru, dan mengontrol kunci dan nilai tanda mana yang ditetapkan pada sumber daya Anda.

Untuk mengontrol kunci dan nilai tag mana yang ditetapkan pada sumber daya yang ada, Anda dapat menerapkan izin tingkat sumber daya ke tindakan `UntagResource` Amazon FSx API dalam kebijakan IAM Anda. `TagResource`

Untuk informasi lebih lanjut tentang izin yang diperlukan untuk memberi tag pada sumber daya Amazon FSx saat pembuatan, lihat. Memberikan izin untuk memberi tanda pada sumber daya saat sumber daya tersebut dibuat

Untuk informasi selengkapnya tentang cara menggunakan tanda untuk membatasi akses ke sumber daya Amazon FSx dalam kebijakan IAM, lihat. Menggunakan tag untuk mengontrol akses ke sumber daya Amazon FSx Anda

Untuk informasi tentang penandaan sumber daya Anda untuk penagihan, lihat Menggunakan tanda alokasi biaya dalam Buku Panduan. AWS Billing

Menyalin tag ke cadangan

Saat Anda membuat atau memperbarui volume di Amazon FSx API atauAWS CLI, Anda dapat mengaktifkan `CopyTagsToBackups` untuk secara otomatis menyalin tag apa pun dari volume Anda ke cadangan.

> **Note**
>
> Jika Anda menentukan tag saat membuat cadangan yang dimulai pengguna (termasuk tag nama saat Anda membuat cadangan menggunakan konsol Amazon FSx), tag tidak akan disalin dari volume meskipun Anda telah mengaktifkannya. `CopyTagsToBackups`

Untuk informasi lebih lanjut tentang pencadangan, lihat. Menggunakan cadangan Untuk informasi selengkapnya tentang mengaktifkan`CopyTagsToBackups`, lihat Untuk membuat volume (CLI) dan Untuk memperbarui konfigurasi volume (CLI) di Panduan Pengguna Amazon FSx for NetApp ONTAP atau CreateVolumedan UpdateVolumedalam Referensi API Amazon FSx for ONTAP. NetApp

Pembatasan tanda

Batasan dasar berikut berlaku untuk tanda:

- Jumlah maksimum tag per sumber daya adalah 50.
- Panjang kunci maksimum adalah 128 karakter Unicode dalam UTF-8.
- Panjang nilai maksimum adalah 256 karakter Unicode dalam UTF-8.
- Karakter yang diizinkan adalah huruf, angka, dan spasi yang dapat diwakili dalam UTF-8, dan karakter berikut: `+ - ` (tanda hubung) (garis bawah). `= . _ : / @`
- Untuk setiap sumber daya, setiap kunci tanda harus unik, dan setiap kunci tanda hanya dapat memiliki satu nilai.
- Kunci dan nilai tag peka huruf besar dan kecil.
- Prefiks `aws:` disimpan untuk penggunaan AWS. Jika sebuah tag memiliki sebuah kunci tag dengan prefiks ini, Anda tidak dapat mengedit atau menghapus kunci atau nilai tanda tersebut. Tanda dengan prefiks `aws:` tidak mengurangi batas tanda per batas sumber daya Anda.

Anda tidak dapat menghapus sumber daya hanya karena tanda saja; Anda harus menentukan pengidentifikasi sumber daya. Misalnya, untuk menghapus sistem file yang Anda beri tag dengan tanda kunci yang disebut`DeleteMe`, Anda harus menggunakan `DeleteFileSystem` tindakan tersebut dengan pengidentifikasi sumber daya sistem file, misalnya. `fs-1234567890abcdef0`

Saat Anda memberi tag pada sumber daya publik atau berbagi, tanda yang Anda berikan hanya tersediaAkun AWS; tidak ada yang Akun AWS memiliki akses ke tanda tersebut. Untuk kontrol akses berbasis tanda ke sumber daya bersama, masing-masing Akun AWS harus tetapkan kumpulan tandanya sendiri untuk mengontrol akses ke sumber daya.

Izin dan penandaan

Untuk informasi lebih lanjut tentang izin yang diperlukan untuk memberi tag pada sumber daya Amazon FSx saat pembuatan, lihat. Memberikan izin untuk memberi tanda pada sumber daya saat sumber daya tersebut dibuat

Untuk informasi selengkapnya tentang cara menggunakan tanda untuk membatasi akses ke sumber daya Amazon FSx dalam kebijakan IAM, lihat. Menggunakan tag untuk mengontrol akses ke sumber daya Amazon FSx Anda

Mengelola FSx untuk sumber daya ONTAP menggunakan aplikasi NetApp

Selain AWS Management Console,, dan AWS API dan SDK AWS CLI, Anda juga dapat menggunakan alat dan aplikasi NetApp manajemen ini untuk mengelola FSx Anda untuk sumber daya ONTAP:

Topik

- Mendaftar untuk NetApp akun
- Menggunakan NetApp BlueXP
- Menggunakan CLI NetApp ONTAP
- Menggunakan ONTAP REST API

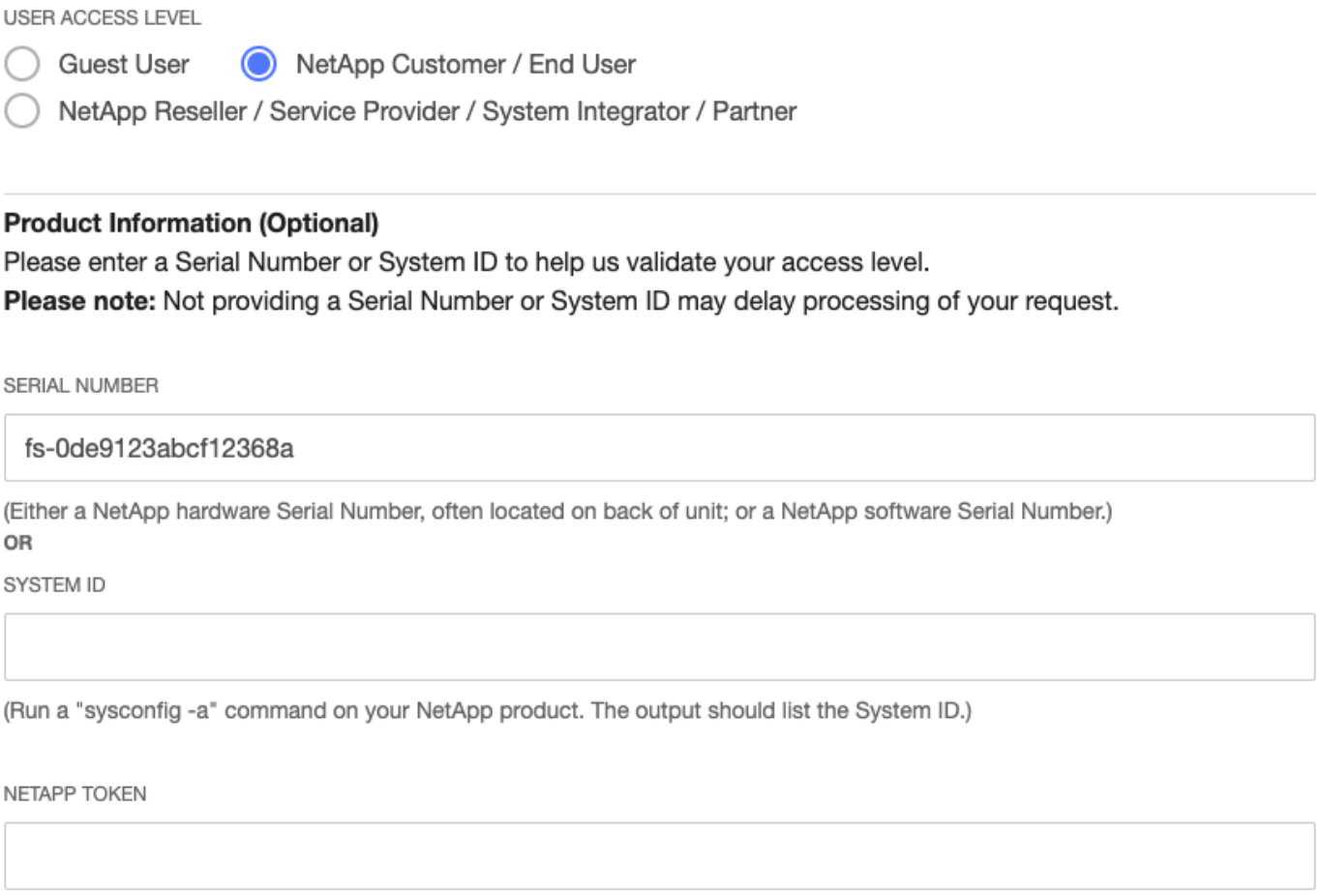
> **Important**
>
> Amazon FSx secara berkala disinkronkan dengan ONTAP untuk memastikan konsistensi. Jika Anda membuat atau memodifikasi volume menggunakan NetApp aplikasi, mungkin

diperlukan waktu hingga beberapa menit agar perubahan ini tercermin dalam API AWS Management Console, AWS CLI, dan SDK.

Mendaftar untuk NetApp akun

Untuk mengunduh beberapa NetApp perangkat lunak, sepertiBlueXP,SnapCenter, dan konektor ONTAP Antivirus, Anda harus memiliki NetApp akun. Untuk mendaftar NetApp akun, lakukan langkah-langkah berikut:

1. Buka halaman Pendaftaran NetApp Pengguna dan daftar untuk akun NetApp pengguna baru.
2. Lengkapi formulir dengan informasi Anda. Pastikan untuk memilih tingkat akses NetAppCustomer/End User. Di bidang SERIAL NUMBER, salin dan tempel ID Sistem File untuk FSx Anda untuk sistem file ONTAP. Lihat contoh berikut ini:



Apa yang diharapkan setelah Anda mendaftar

Pelanggan dengan NetApp produk yang sudah ada akan memiliki akun NSS mereka naik level ke akses Tingkat Pelanggan dalam satu hari kerja. Pelanggan baru NetApp akan dionboard menggunakan praktik bisnis standar, selain memiliki akun NSS mereka yang ditingkatkan ke akses Tingkat Pelanggan. Menyediakan ID Sistem File membantu mempercepat proses ini. Anda dapat memeriksa status akun NSS Anda dengan masuk ke mysupport.netapp.com dan menavigasi ke halaman Selamat Datang. Tingkat akses akun Anda harus Akses Pelanggan.

Menggunakan NetApp BlueXP

NetApp BlueXP adalah bidang kontrol terpadu yang menyederhanakan pengalaman manajemen untuk penyimpanan dan layanan data di lingkungan lokal dan cloud. BlueXP menyediakan antarmuka pengguna terpusat untuk mengelola, memantau, dan mengotomatiskan penerapan ONTAP di dalam dan di tempat. AWS Untuk informasi selengkapnya, lihat dokumentasi NetApp BlueXP dan dokumentasi NetApp BlueXP untuk Amazon fsX untuk ONTAP. NetApp

> **Note**
>
> NetApp BlueXPtidak didukung untuk sistem file scale-out.

Menggunakan NetApp System Manager dengan BlueXP

Anda dapat mengelola Amazon FSx untuk sistem file NetApp ONTAP menggunakan System Manager langsung dari. BlueXP BlueXPmemungkinkan Anda menggunakan antarmuka Manajer Sistem yang sama dengan yang biasa Anda gunakan, sehingga Anda dapat mengelola infrastruktur multi-cloud hybrid Anda dari satu bidang kontrol. Anda juga memiliki akses ke fungsi BlueXP lainnya. Untuk informasi selengkapnya, lihat topik Integrasi Manajer Sistem dengan BlueXP di dokumentasi NetApp ONTAP.

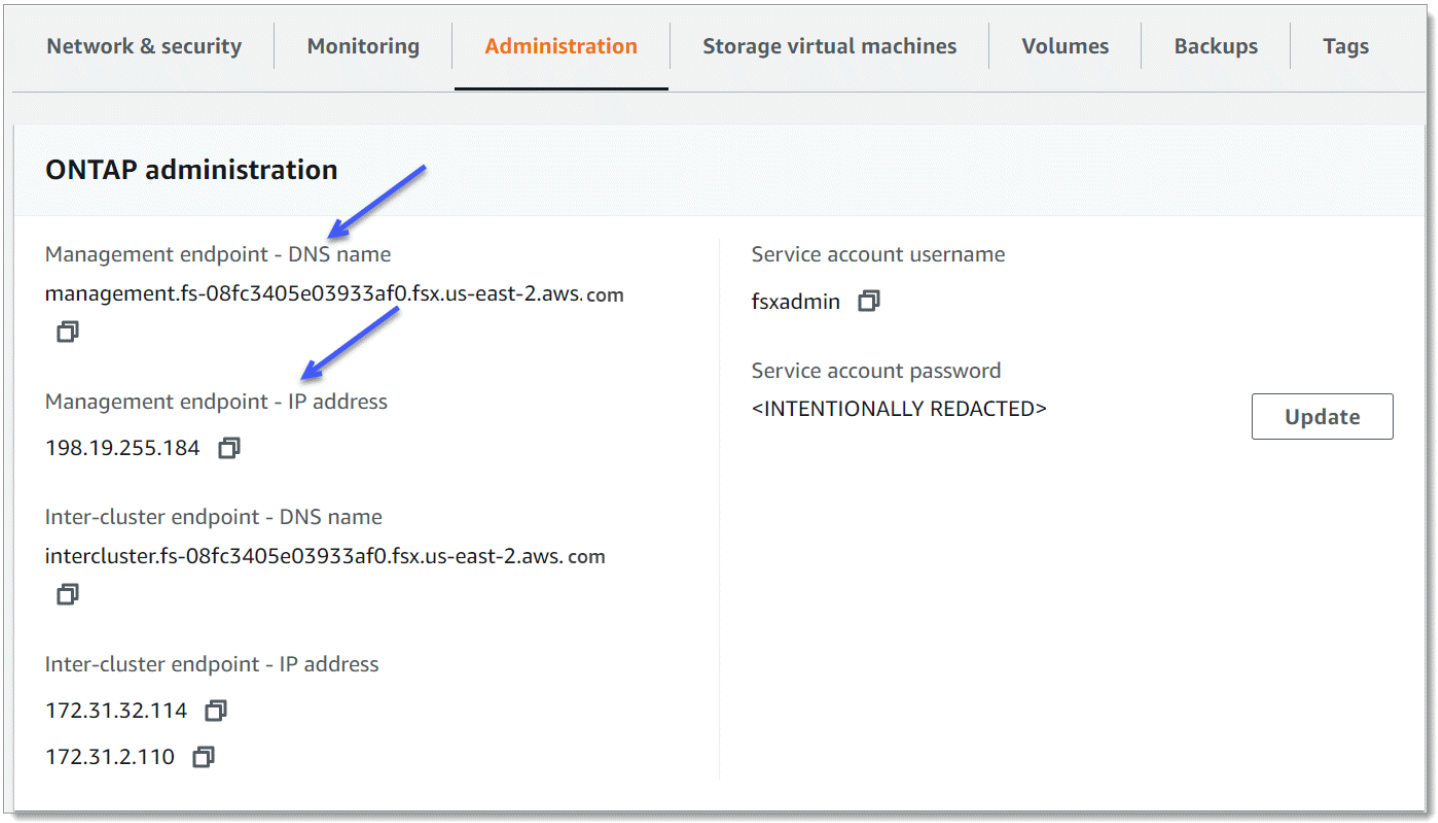
> **Note**
>
> NetApp Manajer Sistem tidak didukung untuk sistem file scale-out.

Menggunakan CLI NetApp ONTAP

Anda dapat mengelola Amazon FSx Anda untuk sumber daya NetApp ONTAP menggunakan CLI. NetApp ONTAP Anda dapat mengelola sumber daya di tingkat sistem file (analog dengan cluster NetApp ONTAP), dan pada tingkat SVM.

Mengelola sistem file dengan ONTAP CLI

Anda dapat menjalankan perintah ONTAP CLI pada FSx Anda untuk sistem file ONTAP, analog dengan menjalankannya di cluster. NetApp ONTAP Anda mengakses ONTAP CLI pada sistem file Anda dengan membuat koneksi shell aman (SSH) ke titik akhir manajemen sistem file, masuk dengan nama pengguna dan kata sandi. `fsxadmin` Anda memiliki opsi untuk mengatur kata sandi saat Anda membuat sistem file menggunakan alur pembuatan kustom atau menggunakan AWS CLI. Jika Anda membuat sistem file menggunakan opsi Buat Cepat, `fsxadmin` kata sandi tidak disetel, jadi Anda harus menyetelnya untuk masuk ke CLI ONTAP. Untuk informasi selengkapnya, lihat Memperbarui sistem file. Anda dapat menemukan nama DNS dan alamat IP titik akhir manajemen sistem file Anda di konsol Amazon FSx, di tab Administrasi halaman detail sistem file fsX untuk ONTAP, yang ditunjukkan pada grafik berikut.



Untuk terhubung ke endpoint manajemen sistem file dengan SSH, gunakan `fsxadmin` pengguna dan kata sandi. Anda dapat SSH ke alamat IP endpoint manajemen sistem file atau nama DNS dari klien yang berada di VPC yang sama dengan sistem file, seperti pada contoh berikut.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

Perintah SSH dengan nilai sampel:

```
ssh fsxadmin@198.51.100.0
```

Perintah SSH menggunakan nama DNS endpoint manajemen:

```
ssh fsxadmin@file-system-management-endpoint-dns-name
```

Perintah SSH menggunakan contoh nama DNS:

```
$ ssh fsxadmin@management.fs-0abcdef123456789.fsx.us-east-2.aws.com
  Password: fsxadmin-password

This is your first recorded login.
FsxId0abcdef123456789::>
```

Lingkup perintah ONTAP CLI tersedia untuk **`fsxadmin`**

Tampilan administratif berada pada tingkat sistem file, yang mencakup semua SVM dan volume dalam sistem file. `fsxadmin` `fsxadmin`Peran melakukan peran administrator ONTAP cluster. Karena Amazon FSx untuk sistem file NetApp ONTAP sepenuhnya dikelola, `fsxadmin` peran dapat menjalankan subset dari perintah CLI yang tersedia. ONTAP

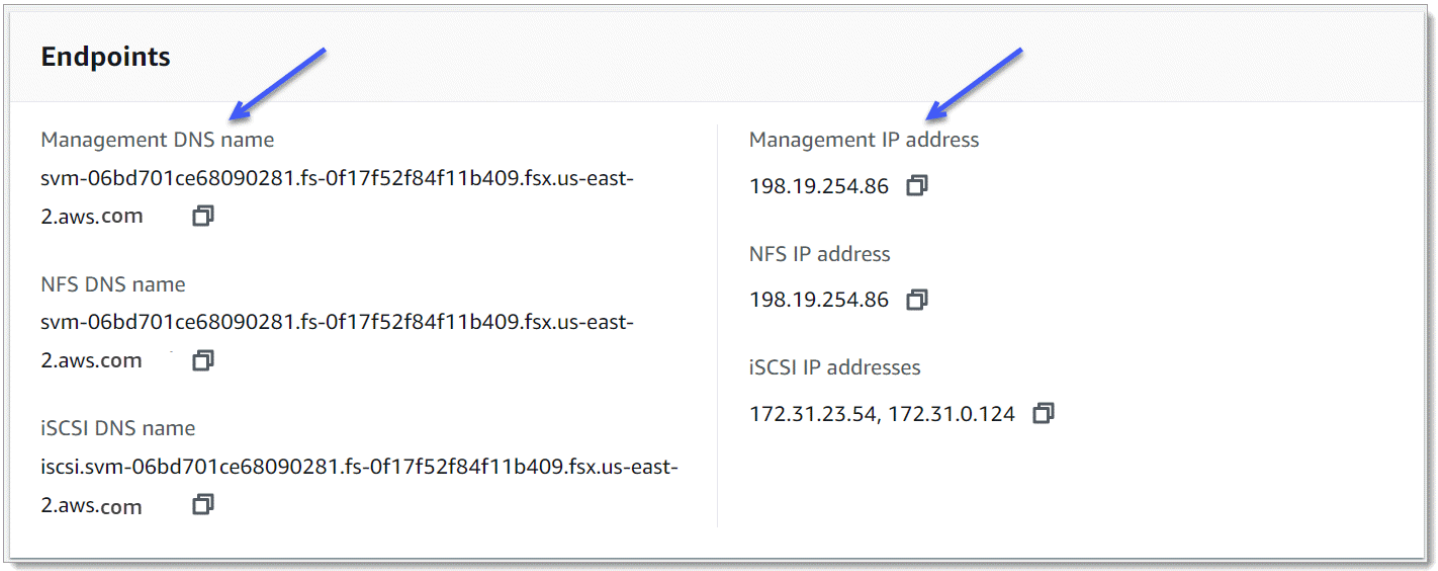
Untuk melihat daftar perintah yang `fsxadmin` dapat dijalankan, gunakan perintah `security login role show`ONTAPCLI berikut:

```
FsxId0abc123def456::> security login role show -role fsxadmin -access !none
           Role          Command/                                  Access
Vserver    Name          Directory                        Query Level
---------- ------------- --------- ---------------------------------- --------
FsxId0abcdef123456789
           fsxadmin      application                                 all
```

```
                        cluster application-record                    all
                        cluster date show                             readonly
                        cluster ha modify                             readonly
                        cluster ha show                               readonly
                        cluster identity modify                       readonly
                        cluster identity show                         readonly
                        cluster log-forwarding           -port !55555 all
                        cluster modify                                readonly
                        cluster peer                                  all
                        cluster show                                  readonly
                        cluster statistics show                       readonly
                        cluster time-service ntp server create        readonly
                        cluster time-service ntp server delete        readonly
                        cluster time-service ntp server modify        readonly
                        cluster time-service ntp server show          readonly
                        debug network tcpdump       -ipspace !Cluster all
                        debug san lun                                 all
                        df         -vserver !FsxId* -vserver !Cluster readonly
                        echo                                          all
                        event catalog show                            readonly
                        event config                                  all
.
.
.
363 entries were displayed.
```

Mengelola SVM dengan CLI ONTAP

Anda dapat mengakses ONTAP CLI di SVM Anda dengan membuat koneksi shell aman (SSH) ke titik akhir manajemen SVM menggunakan `fsxadmin` atau nama pengguna dan kata sandi. `vsadmin` Anda dapat menemukan nama DNS endpoint manajemen SVM dan alamat IP di konsol Amazon FSx, di panel Endpoints pada halaman detail mesin virtual Penyimpanan, yang ditunjukkan pada grafik berikut.



Untuk terhubung ke titik akhir manajemen SVM dengan SSH, Anda dapat menggunakan `fsxadmin` nama pengguna `vsadmin` atau kata sandi. Jika Anda tidak menetapkan kata sandi untuk `vsadmin` pengguna saat SVM dibuat, Anda dapat mengatur `vsadmin` kata sandi kapan saja. Untuk informasi selengkapnya, lihat Memperbarui mesin virtual penyimpanan. Anda dapat SSH ke SVM dari klien yang berada di VPC yang sama dengan sistem file, menggunakan alamat IP endpoint manajemen atau nama DNS.

```
ssh vsadmin@svm-management-endpoint-ip-address
```

Perintah dengan nilai sampel:

```
ssh vsadmin@198.51.100.10
```

Perintah SSH menggunakan nama DNS endpoint manajemen:

```
ssh vsadmin@svm-management-endpoint-dns-name
```

Perintah SSH menggunakan contoh nama DNS:

```
ssh vsadmin@management.svm-abcdef01234567892fs-0abcdef123456789.fsx.us-east-2.aws.com
```

```
Password: vsadmin-password

This is your first recorded login.
```

```
FsxId0abcdef123456789::>
```

Amazon FSx untuk NetApp ONTAP mendukung perintah CLINetApp ONTAP.

Untuk referensi lengkap perintah NetApp ONTAP CLI, lihat Perintah ONTAP: Referensi Halaman Manual.

Menggunakan ONTAP REST API

Saat mengakses fsX Anda untuk sistem file ONTAP menggunakan REST API menggunakan ONTAP kredensyal, `fsxadmin` lakukan salah satu hal berikut:

- Nonaktifkan validasi TLS.

  Atau

- Percayai otoritas AWS sertifikat (CA) - Bundel sertifikat untuk CA di setiap wilayah dapat ditemukan di URL berikut:
  - https://fsx-aws-certificates.s3.amazonaws.com/bundle - *`aws-region`* .pem untuk Publik Wilayah AWS
  - https://fsx-aws-us-gov-certificates.s3.us-gov-west-1.amazonaws.com/bundle - *`aws-region`* .pem untuk Wilayah AWS GovCloud
  - https://fsx-aws-cn-certificates.s3.cn-north-1.amazonaws.com.cn/bundle - *`aws-region`* .pem untuk Wilayah China AWS

Untuk referensi lengkap perintah NetApp ONTAP REST API, lihat Referensi Online NetApp ONTAP REST API.

Keamanan di Amazon FSx untuk ONTAP NetApp

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon FSx untuk NetApp ONTAP, lihat AWS Layanan dalam Lingkup menurut Program Kepatuhan dalam Lingkup oleh Program Kepatuhan.
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Amazon FSx. Topik berikut menunjukkan cara mengonfigurasi Amazon FSx untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Amazon FSx Anda.

Topik

- Peran dan pengguna di Amazon FSx untuk ONTAP NetApp

Perlindungan data di Amazon FSx untuk ONTAP NetApp

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di Amazon FSx untuk NetApp ONTAP. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensil dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Amazon FSx atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan

atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Enkripsi data di FSx untuk ONTAP

Amazon FSx untuk NetApp ONTAP mendukung enkripsi data saat istirahat dan enkripsi data dalam perjalanan. Enkripsi data at rest secara otomatis akan diaktifkan saat membuat sistem file Amazon FSx. Amazon FSx untuk NetApp ONTAP mendukung enkripsi berbasis KerberOS dalam perjalanan melalui protokol NFS dan SMB jika Anda mengakses data di Storage Virtual Machine (SVM) yang digabungkan ke Active Directory atau ke domain menggunakan Lightweight Directory Access Protocol (LDAP).

Kapan menggunakan enkripsi

Jika organisasi Anda tunduk pada kebijakan perusahaan atau peraturan yang memerlukan enkripsi data dan metadata saat istirahat, data Anda secara otomatis dienkripsi saat istirahat. Kami juga menyarankan Anda mengaktifkan enkripsi data dalam perjalanan dengan memasang sistem file Anda menggunakan enkripsi data dalam perjalanan.

Untuk informasi selengkapnya tentang enkripsi data dengan Amazon FSx untuk NetApp ONTAP, lihat dan. Enkripsi data saat tidak digunakan Mengenkripsi data dalam perjalanan

Enkripsi data saat tidak digunakan

Semua Amazon FSx untuk sistem file NetApp ONTAP dienkripsi saat istirahat dengan kunci yang dikelola menggunakan (). AWS Key Management Service AWS KMS Data dienkripsi secara otomatis sebelum ditulis ke sistem file, dan secara otomatis didekripsi saat dibaca. Proses ini ditangani secara transparan oleh Amazon FSx, sehingga Anda tidak perlu memodifikasi aplikasi Anda.

Amazon FSx menggunakan algoritme enkripsi AES-256 standar industri untuk mengenkripsi data dan metadata Amazon FSx saat istirahat. Untuk informasi selengkapnya, lihat Dasar-dasar kriptografi dalam Panduan Developer AWS Key Management Service .

> **Note**
>
> Infrastruktur manajemen AWS kunci menggunakan Federal Information Processing Standards (FIPS) 140-2 algoritma kriptografi yang disetujui. Infrastruktur ini konsisten dengan rekomendasi National Institute of Standard and Technology (NIST) 800-57.

Bagaimana Amazon FSx menggunakan AWS KMS

Amazon FSx terintegrasi dengan AWS KMS untuk manajemen kunci. Amazon FSx menggunakan kunci KMS untuk mengenkripsi sistem file Anda. Anda memilih kunci KMS yang digunakan untuk mengenkripsi dan mendekripsi sistem file (baik data maupun metadata). Anda dapat mengaktifkan, menonaktifkan, atau mencabut hibah pada kunci KMS ini. Kunci KMS ini dapat menjadi salah satu dari dua jenis berikut:

- AWS-Managed KMS key - Ini adalah kunci KMS default, dan gratis untuk digunakan.
- Kunci KMS yang dikelola pelanggan - Ini adalah kunci KMS yang paling fleksibel untuk digunakan, karena Anda dapat mengonfigurasi kebijakan dan hibah utamanya untuk beberapa pengguna atau layanan. Untuk informasi selengkapnya tentang membuat kunci KMS, lihat Membuat Kunci di Panduan AWS Key Management Service Pengembang.

> **Important**
>
> Amazon FSx hanya menerima kunci KMS enkripsi simetris. Anda tidak dapat menggunakan kunci KMS asimetris dengan Amazon FSx.

Jika Anda menggunakan kunci KMS yang dikelola pelanggan sebagai kunci KMS Anda untuk enkripsi dan dekripsi data file, Anda dapat mengaktifkan rotasi kunci. Bila Anda mengaktifkan rotasi kunci, AWS KMS secara otomatis akan merotasi kunci Anda satu kali per tahun. Selain itu, dengan kunci KMS yang dikelola pelanggan, Anda dapat memilih kapan harus menonaktifkan, mengaktifkan kembali, menghapus, atau mencabut akses ke kunci KMS Anda kapan saja. Untuk informasi selengkapnya, lihat Memutar AWS KMS keys dan Mengaktifkan dan menonaktifkan kunci di Panduan Pengembang.AWS Key Management Service

Kebijakan utama Amazon FSx untuk AWS KMS

Kebijakan utama adalah cara utama untuk mengontrol akses ke kunci KMS. Untuk informasi selengkapnya tentang kebijakan kunci, lihat Menggunakan kebijakan kunci di AWS KMS dalam Panduan Developer AWS Key Management Service . Daftar berikut menjelaskan semua izin AWS KMS terkait yang didukung oleh Amazon FSx untuk sistem file terenkripsi saat istirahat:

- kms:Encrypt – (Opsional) Mengenkripsi plaintext ke ciphertext. Izin ini termasuk dalam kebijakan kunci default.

- kms:Decrypt – (Wajib) Mendekripsi ciphertext. Ciphertext adalah teks biasa yang sebelumnya telah dienkripsi. Izin ini termasuk dalam kebijakan kunci default.
- kms: ReEncrypt — (Opsional) Mengenkripsi data di sisi server dengan yang baru AWS KMS key, tanpa mengekspos plaintext data di sisi klien. Data pertama kali didekripsi dan kemudian dienkripsi ulang. Izin ini termasuk dalam kebijakan kunci default.
- kms: GenerateData KeyWithout Plaintext — (Diperlukan) Mengembalikan kunci enkripsi data yang dienkripsi di bawah kunci KMS. Izin ini disertakan dalam kebijakan kunci default di bawah kms: GenerateData Key*.
- kms: CreateGrant — (Diperlukan) Menambahkan hibah ke kunci untuk menentukan siapa yang dapat menggunakan kunci dan dalam kondisi apa. Hibah adalah mekanisme izin lainnya untuk kebijakan kunci. Untuk informasi lebih lanjut tentang hibah, lihat Menggunakan Pemberian di Panduan Developer AWS Key Management Service . Izin ini termasuk dalam kebijakan kunci default.
- kms: DescribeKey - (Diperlukan) Memberikan informasi rinci tentang kunci KMS yang ditentukan. Izin ini termasuk dalam kebijakan kunci default.
- kms: ListAliases — (Opsional) Daftar semua alias kunci di akun. Saat Anda menggunakan konsol untuk membuat sistem file terenkripsi, izin ini mengisi daftar kunci KMS. Kami merekomendasikan untuk menggunakan izin ini untuk memberikan pengalaman pengguna yang terbaik. Izin ini termasuk dalam kebijakan kunci default.

Mengenkripsi data dalam perjalanan

Topik ini menjelaskan berbagai opsi yang tersedia untuk mengenkripsi data file Anda saat sedang dalam perjalanan antara sistem file FSx untuk ONTAP dan klien yang terhubung. Ini juga memberikan panduan untuk membantu Anda memilih metode enkripsi mana yang paling cocok untuk alur kerja Anda.

Semua data yang mengalir di Wilayah AWS seluruh jaringan AWS global secara otomatis dienkripsi pada lapisan fisik sebelum meninggalkan fasilitas yang AWS aman. Semua lalu lintas antara Availability Zones dienkripsi. Lapisan enkripsi tambahan, termasuk yang tercantum di bagian ini, memberikan perlindungan tambahan. Untuk informasi selengkapnya tentang cara AWS menyediakan perlindungan untuk data yang mengalir di seluruh Zona Tersedia Wilayah AWS, dan instans, lihat Enkripsi saat transit di Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Linux.

Amazon FSx untuk NetApp ONTAP mendukung metode berikut untuk mengenkripsi data dalam perjalanan antara fsX untuk sistem file ONTAP dan klien yang terhubung:

- Enkripsi berbasis Nitro otomatis atas semua protokol dan klien yang didukung yang berjalan pada jenis instans Amazon EC2 Linux dan Windows yang didukung.
- Enkripsi berbasis Kerberos melalui protokol NFS dan SMB.
- Enkripsi berbasis IPsec melalui protokol NFS, iSCSI, dan SMB

Semua metode yang didukung untuk mengenkripsi data dalam perjalanan menggunakan algoritme kriptografi AES-256 standar industri yang menyediakan enkripsi kekuatan perusahaan.

Topik

- Memilih metode untuk mengenkripsi data dalam perjalanan
- Mengenkripsi data dalam perjalanan dengan AWS Sistem Nitro
- Mengenkripsi data dalam perjalanan dengan enkripsi berbasis Kerberos
- Mengenkripsi data dalam perjalanan dengan enkripsi IPsec
- Aktifkan enkripsi data SMB dalam perjalanan
- Mengkonfigurasi IPsec menggunakan otentikasi PSK
- Mengkonfigurasi IPsec menggunakan otentikasi sertifikat

Memilih metode untuk mengenkripsi data dalam perjalanan

Bagian ini memberikan informasi yang dapat membantu Anda memutuskan enkripsi mana yang didukung dalam metode transit yang terbaik untuk alur kerja Anda. Lihat kembali bagian ini saat Anda menjelajahi opsi yang didukung yang dijelaskan secara rinci di bagian berikut.

Ada beberapa faktor yang perlu dipertimbangkan ketika memilih bagaimana Anda akan mengenkripsi data dalam perjalanan antara FSx Anda untuk sistem file ONTAP dan klien yang terhubung. Faktor-faktor ini meliputi:

- Sistem file FSx untuk ONTAP Anda berjalan. Wilayah AWS
- Jenis instance yang dijalankan klien.
- Lokasi klien mengakses sistem file Anda.
- Persyaratan kinerja jaringan.
- Protokol data yang ingin Anda enkripsi.
- Jika Anda menggunakan Microsoft Active Directory.

Wilayah AWS

Sistem file Anda berjalan menentukan apakah Anda dapat menggunakan enkripsi berbasis Amazon Nitro atau tidak. Wilayah AWS Enkripsi berbasis Nitro tersedia sebagai berikut: Wilayah AWS

- AS Timur (N. Virginia)
- AS Timur (Ohio)
- AS Barat (Oregon)
- Eropa (Irlandia)

Selain itu, enkripsi berbasis Nitro tersedia untuk sistem file scale-out di Asia Pasifik (Sydney). Wilayah AWS

Jenis contoh klien

Anda dapat menggunakan enkripsi berbasis Amazon Nitro jika klien yang mengakses sistem file Anda berjalan di salah satu jenis instans Amazon EC2 Mac, Linux, atau Windows yang didukung, dan alur kerja Anda memenuhi semua persyaratan lain untuk menggunakan enkripsi berbasis Nitro. Tidak ada persyaratan tipe instance klien untuk menggunakan enkripsi Kerberos atau IPsec.

Lokasi klien

Lokasi klien yang mengakses data sehubungan dengan lokasi sistem file Anda memengaruhi metode enkripsi in-transit yang tersedia untuk digunakan. Anda dapat menggunakan salah satu metode enkripsi yang didukung jika klien dan sistem file berada di VPC yang sama. Hal yang sama berlaku jika klien dan sistem file berada di VPC peered, selama lalu lintas tidak melewati perangkat atau layanan jaringan virtual, seperti gateway transit. Enkripsi berbasis Nitro bukanlah pilihan yang tersedia jika klien tidak berada dalam VPC yang sama atau diintip, atau jika lalu lintas melewati perangkat atau layanan jaringan virtual.

Performa jaringan

Menggunakan enkripsi berbasis Amazon Nitro tidak berdampak pada kinerja jaringan. Ini karena instans Amazon EC2 yang didukung menggunakan kemampuan pembongkaran perangkat keras Sistem Nitro yang mendasarinya untuk secara otomatis mengenkripsi lalu lintas dalam transit antar instans.

Menggunakan enkripsi Kerberos atau IPsec berdampak pada kinerja jaringan. Ini karena kedua metode enkripsi ini berbasis perangkat lunak, yang mengharuskan klien dan server untuk menggunakan sumber daya komputasi untuk mengenkripsi dan mendekripsi lalu lintas dalam transit.

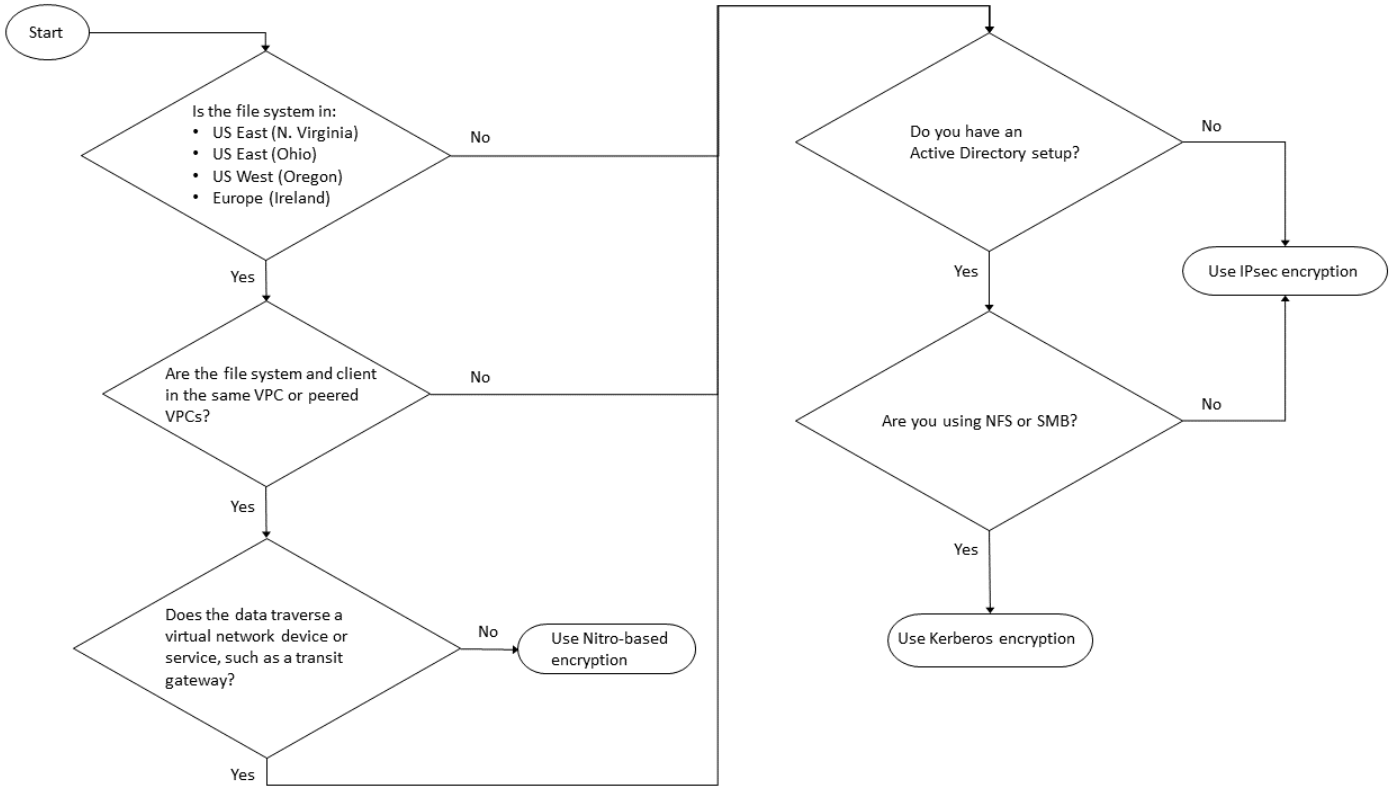
Protokol data

Anda dapat menggunakan enkripsi berbasis Amazon Nitro dan enkripsi IPSec dengan semua protokol yang didukung — NFS, SMB, dan iSCSI. Anda dapat menggunakan enkripsi Kerberos dengan protokol NFS dan SMB (dengan Active Directory).

Direktori Aktif

Jika Anda menggunakan Microsoft Active Directory, Anda dapat menggunakan enkripsi Kerberos melalui protokol NFS dan SMB.

Gunakan diagram berikut untuk membantu Anda memutuskan metode enkripsi dalam transit mana yang akan digunakan.



Enkripsi IPsec adalah satu-satunya pilihan yang tersedia ketika semua kondisi berikut berlaku untuk alur kerja Anda:

- Anda menggunakan protokol NFS, SMB, atau iSCSI.
- Alur kerja Anda tidak mendukung penggunaan enkripsi berbasis Amazon Nitro.
- Anda tidak menggunakan domain Microsoft Active Directory.

Mengenkripsi data dalam perjalanan dengan AWS Sistem Nitro

Dengan enkripsi berbasis Nitro, data dalam transit dienkripsi secara otomatis saat klien yang mengakses sistem file Anda berjalan pada jenis instans Amazon EC2 Linux atau Windows yang didukung.

Menggunakan enkripsi berbasis Amazon Nitro tidak berdampak pada kinerja jaringan. Ini karena instans Amazon EC2 yang didukung menggunakan kemampuan pembongkaran perangkat keras Sistem Nitro yang mendasarinya untuk secara otomatis mengenkripsi lalu lintas dalam transit antar instans.

Enkripsi berbasis Nitro diaktifkan secara otomatis ketika jenis instance klien yang didukung berada di VPC yang sama Wilayah AWS dan di VPC yang sama atau di VPC yang diintip dengan VPC sistem file. Selain itu, jika klien berada dalam VPC peered, maka data tidak dapat melintasi perangkat atau layanan jaringan virtual (seperti gateway transit) agar enkripsi berbasis NITRO diaktifkan secara otomatis. Untuk informasi selengkapnya tentang enkripsi berbasis Nitro, lihat bagian Enkripsi dalam perjalanan dari Panduan Pengguna Amazon EC2 untuk jenis instans Linux atau Windows.

Enkripsi in-transit berbasis Nitro tersedia untuk sistem file yang dibuat setelah 28 November 2022 sebagai berikut: Wilayah AWS

- AS Timur (N. Virginia)
- AS Timur (Ohio)
- AS Barat (Oregon)
- Eropa (Irlandia)

Selain itu, enkripsi berbasis Nitro tersedia untuk sistem file scale-out di Asia Pasifik (Sydney). Wilayah AWS

Untuk informasi selengkapnya tentang Wilayah AWS tempat FSx untuk ONTAP tersedia, lihat Amazon FSx untuk Harga ONTAP. NetApp

Untuk informasi selengkapnya tentang spesifikasi kinerja FSx untuk sistem file ONTAP, lihat. Dampak kapasitas throughput terhadap performa

Mengenkripsi data dalam perjalanan dengan enkripsi berbasis Kerberos

Jika Anda menggunakan Microsoft Active Directory, Anda dapat menggunakan enkripsi berbasis KerberOS melalui protokol NFS dan SMB untuk mengenkripsi data dalam transit untuk volume turunan SVM yang digabungkan ke Microsoft Active Directory.

Mengenkripsi data dalam perjalanan melalui NFS menggunakan Kerberos

Enkripsi data dalam perjalanan menggunakan Kerberos didukung untuk protokol NFSv3 dan NFSv4. Untuk mengaktifkan enkripsi dalam perjalanan menggunakan Kerberos untuk protokol NFS, lihat Menggunakan Kerberos dengan NFS untuk keamanan yang kuat di Pusat Dokumentasi. NetApp ONTAP

Mengenkripsi data dalam perjalanan melalui SMB menggunakan Kerberos

Mengenkripsi data dalam perjalanan melalui protokol SMB didukung pada berbagi file yang dipetakan pada instance komputasi yang mendukung protokol SMB 3.0 atau yang lebih baru. Ini termasuk semua Microsoft Windows versi dari Microsoft Windows Server 2012 dan yang lebih baru, dan Microsoft Windows 8 dan yang lebih baru. Saat diaktifkan, FSx untuk ONTAP secara otomatis mengenkripsi data dalam perjalanan menggunakan enkripsi SMB saat Anda mengakses sistem file Anda tanpa perlu memodifikasi aplikasi Anda.

FSx untuk ONTAP SMB mendukung enkripsi 128 dan 256 bit, yang ditentukan oleh permintaan sesi klien. Untuk deskripsi tingkat enkripsi yang berbeda, lihat bagian Mengatur tingkat keamanan otentikasi minimum server SMB dari Kelola SMB dengan CLI di Pusat Dokumentasi. NetApp ONTAP

> **Note**
>
> Klien menentukan algoritma enkripsi. Otentikasi NTLM dan Kerberos bekerja dengan enkripsi 128 dan 256 bit. FSx untuk ONTAP SMB Server menerima semua permintaan klien Windows standar, dan kontrol granular ditangani oleh Kebijakan Grup Microsoft atau pengaturan Registri.

Anda menggunakan ONTAP CLI untuk mengelola enkripsi dalam pengaturan transit di FSx untuk ONTAP SVM dan volume. Untuk mengakses NetApp ONTAP CLI, buat sesi SSH pada SVM tempat Anda membuat enkripsi dalam pengaturan transit, seperti yang dijelaskan dalam. Mengelola SVM dengan CLI ONTAP

Untuk petunjuk tentang cara mengaktifkan enkripsi SMB pada SVM atau volume, lihat. Aktifkan enkripsi data SMB dalam perjalanan

Mengenkripsi data dalam perjalanan dengan enkripsi IPsec

FSx untuk ONTAP mendukung penggunaan protokol IPsec dalam mode transportasi untuk memastikan data terus aman dan terenkripsi, saat dalam perjalanan. IPSec menawarkan end-to-end enkripsi data dalam transit antara klien dan FSx untuk sistem file ONTAP untuk semua lalu lintas IP yang didukung - protokol NFS, iSCSI, dan SMB. Dengan enkripsi IPsec, Anda membuat terowongan IPsec antara FSx untuk ONTAP SVM yang dikonfigurasi dengan IPSec diaktifkan, dan klien IPsec yang berjalan pada klien yang terhubung mengakses data.

Kami menyarankan Anda menggunakan IPSec untuk mengenkripsi data dalam perjalanan melalui protokol NFS, SMB, dan iSCSI saat mengakses data Anda dari klien yang tidak mendukung enkripsi berbasis NITRO, dan jika klien dan SVM Anda tidak bergabung ke Active Directory, yang diperlukan untuk enkripsi berbasis KerberOS. Enkripsi IPsec adalah satu-satunya pilihan yang tersedia untuk mengenkripsi data dalam perjalanan untuk lalu lintas iSCSI ketika klien iSCSI Anda tidak mendukung enkripsi berbasis Nitro.

Untuk autentikasi IPsec, Anda dapat menggunakan kunci pra-bersama (PSK) atau sertifikat. Jika Anda menggunakan PSK, klien IPsec yang Anda gunakan harus mendukung Internet Key Exchange versi 2 (IKEv2) dengan PSK. Langkah-langkah tingkat tinggi untuk mengkonfigurasi enkripsi IPsec pada FSx untuk ONTAP dan klien adalah sebagai berikut:

1. Aktifkan dan konfigurasikan IPsec pada sistem file Anda.
2. Instal dan konfigurasikan IPsec pada klien Anda
3. Konfigurasikan IPsec untuk beberapa akses klien

Untuk informasi selengkapnya tentang cara mengonfigurasi IPsec menggunakan PSK, lihat Mengkonfigurasi keamanan IP (IPsec) melalui enkripsi kawat di pusat dokumentasi. NetApp ONTAP

Untuk informasi selengkapnya tentang cara mengonfigurasi IPsec menggunakan sertifikat, lihatMengkonfigurasi IPsec menggunakan otentikasi sertifikat.

Aktifkan enkripsi data SMB dalam perjalanan

Secara default, saat Anda membuat SVM, enkripsi SMB dimatikan. Anda dapat mengaktifkan enkripsi SMB yang diperlukan pada saham individu, atau pada SVM, yang menyalakannya untuk semua saham di SVM tersebut.

> **Note**
>
> Ketika enkripsi SMB yang diperlukan diaktifkan pada SVM atau berbagi, klien SMB yang tidak mendukung enkripsi tidak dapat terhubung ke SVM atau berbagi itu.

Untuk memerlukan enkripsi SMB untuk lalu lintas SMB yang masuk pada SVM

Gunakan prosedur berikut untuk meminta enkripsi SMB pada SVM menggunakan CLINetApp ONTAP.

1. Untuk terhubung ke titik akhir manajemen SVM dengan SSH, gunakan nama pengguna `vsadmin` dan kata sandi vsadmin yang Anda atur saat membuat SVM. Jika Anda tidak menetapkan kata sandi vsadmin, gunakan nama pengguna `fsxadmin` dan kata sandi fsxadmin. Anda dapat SSH ke SVM dari klien yang berada di VPC yang sama dengan sistem file, menggunakan alamat IP endpoint manajemen atau nama DNS.

   ```
   ssh vsadmin@svm-management-endpoint-ip-address
   ```

   Perintah dengan nilai sampel:

   ```
   ssh vsadmin@198.51.100.10
   ```

   Perintah SSH menggunakan nama DNS endpoint manajemen:

   ```
   ssh vsadmin@svm-management-endpoint-dns-name
   ```

   Perintah SSH menggunakan contoh nama DNS:

   ```
   ssh vsadmin@management.svm-abcdef01234567892fs-08fc3405e03933af0.fsx.us-
   east-2.aws.com
   ```

   ```
   Password: vsadmin-password

   This is your first recorded login.
   FsxIdabcdef01234567892::>
   ```

2. Gunakan perintah `vserver cifs security modify`NetApp ONTAPCLI untuk meminta enkripsi SMB untuk lalu lintas SMB masuk ke SVM.

```
vserver cifs security modify -vserver vserver_name -is-smb-encryption-required true
```

3. Untuk berhenti memerlukan enkripsi SMB untuk lalu lintas SMB yang masuk, gunakan perintah berikut.

```
vserver cifs security modify -vserver vserver_name -is-smb-encryption-required
 false
```

4. Untuk melihat `is-smb-encryption-required` pengaturan saat ini pada SVM, gunakan perintah `vserver cifs security show`NetApp ONTAPCLI:

```
vserver cifs security show -vserver vs1 -fields is-smb-encryption-required

vserver  is-smb-encryption-required
-------- -------------------------
vs1      true
```

Untuk informasi selengkapnya tentang mengelola enkripsi SMB di SVM, lihat Mengonfigurasi enkripsi SMB yang diperlukan di server SMB untuk transfer data melalui SMB di Pusat Dokumentasi. NetApp ONTAP

Untuk mengaktifkan enkripsi SMB pada volume

Gunakan prosedur berikut untuk mengaktifkan enkripsi SMB pada bagian menggunakan NetApp ONTAP CLI.

1. Buat koneksi shell aman (SSH) ke titik akhir manajemen SVM seperti yang dijelaskan dalam. Mengelola SVM dengan CLI ONTAP
2. Gunakan perintah NetApp ONTAP CLI berikut untuk membuat berbagi SMB baru dan memerlukan enkripsi SMB saat mengakses bagian ini.

```
vserver cifs share create -vserver vserver_name -share-name share_name -
path share_path -share-properties encrypt-data
```

   Untuk informasi selengkapnya, lihat `vserver cifs share create`di halaman manual NetApp ONTAP CLI Command.

3. Untuk memerlukan enkripsi SMB pada berbagi SMB yang ada, gunakan perintah berikut.

```
vserver cifs share properties add -vserver vserver_name -share-name share_name -
share-properties encrypt-data
```

Untuk informasi selengkapnya, lihat vserver cifs share createdi halaman manual NetApp ONTAP CLI Command.

4. Untuk mematikan enkripsi SMB pada berbagi SMB yang ada, gunakan perintah berikut.

```
vserver cifs share properties remove -vserver vserver_name -share-name share_name -
share-properties encrypt-data
```

Untuk informasi selengkapnya, lihat vserver cifs share properties removedi halaman manual NetApp ONTAP CLI Command.

5. Untuk melihat `is-smb-encryption-required` pengaturan saat ini pada berbagi SMB, gunakan perintah NetApp ONTAP CLI berikut:

```
vserver cifs share properties show -vserver vserver_name -share-name share_name -
fields share-properties
```

Jika salah satu properti yang dikembalikan oleh perintah adalah `encrypt-data` properti, maka properti tersebut menentukan bahwa enkripsi SMB harus digunakan saat mengakses share ini.

Untuk informasi selengkapnya, lihat vserver cifs share properties showdi halaman manual NetApp ONTAP CLI Command.

Mengkonfigurasi IPsec menggunakan otentikasi PSK

Jika Anda menggunakan PSK untuk otentikasi, langkah-langkah untuk mengonfigurasi enkripsi IPsec pada FSx untuk ONTAP dan klien adalah sebagai berikut:

1. Aktifkan dan konfigurasikan IPsec pada sistem file Anda.
2. Instal dan konfigurasikan IPsec pada klien Anda
3. Konfigurasikan IPsec untuk beberapa akses klien

Untuk detail tentang mengonfigurasi IPsec menggunakan PSK, lihat Mengkonfigurasi keamanan IP (IPsec) melalui enkripsi kawat di pusat dokumentasi. NetApp ONTAP

Mengkonfigurasi IPsec menggunakan otentikasi sertifikat

Topik berikut memberikan instruksi untuk mengkonfigurasi enkripsi IPsec menggunakan otentikasi sertifikat pada FSx untuk sistem file ONTAP dan klien yang menjalankan Libreswan IPSec. Solusi ini menggunakan AWS Certificate Manager dan AWS Private Certificate Authority membuat otoritas sertifikat pribadi dan untuk menghasilkan sertifikat.

Langkah-langkah tingkat tinggi untuk mengkonfigurasi enkripsi IPsec menggunakan otentikasi sertifikat pada FSx untuk sistem file ONTAP dan klien yang terhubung adalah sebagai berikut:

1. Memiliki otoritas sertifikat untuk menerbitkan sertifikat.
2. Menghasilkan dan mengekspor sertifikat CA untuk sistem file dan klien.
3. Instal sertifikat dan konfigurasikan IPsec pada instance klien.
4. Instal sertifikat dan konfigurasikan IPsec pada sistem file Anda.
5. Tentukan database kebijakan keamanan (SPD).
6. Konfigurasikan IPSec untuk beberapa akses klien.

Membuat dan menginstal sertifikat CA

Untuk otentikasi sertifikat, Anda perlu membuat dan menginstal sertifikat dari otoritas sertifikat pada FSx Anda untuk sistem file ONTAP dan klien yang akan mengakses data pada sistem file Anda. Contoh berikut digunakan AWS Private Certificate Authority untuk mengatur otoritas sertifikat pribadi, dan menghasilkan sertifikat untuk menginstal pada sistem file dan klien. Dengan menggunakan AWS Private Certificate Authority, Anda dapat membuat hierarki root dan subordinate certificate authority (CA) yang sepenuhnya AWS dihosting untuk penggunaan internal oleh organisasi Anda. Proses ini memiliki lima langkah:

1. Membuat Private Certificate Authority (CA) menggunakan AWS Private CA
2. Keluarkan dan instal sertifikat root pada CA pribadi
3. Minta sertifikat pribadi dari AWS Certificate Manager untuk sistem file dan klien Anda
4. Ekspor sertifikat untuk sistem file dan klien.

Untuk informasi selengkapnya, lihat Administrasi CA pribadi di Panduan AWS Private Certificate Authority Pengguna.

Untuk membuat CA pribadi root

1. Saat Anda membuat CA, Anda harus menentukan konfigurasi CA dalam file yang Anda berikan. Perintah berikut menggunakan editor teks Nano untuk membuat `ca_config.txt` file, yang menentukan informasi berikut:

   - Nama algoritme
   - Algoritma penandatanganan yang digunakan CA untuk menandatangani
   - Informasi subjek X.500

   ```
   $ > nano ca_config.txt
   ```

   Editor teks muncul.

2. Edit file dengan spesifikasi untuk CA Anda.

   ```
   {
      "KeyAlgorithm":"RSA_2048",
      "SigningAlgorithm":"SHA256WITHRSA",
      "Subject":{
         "Country":"US",
         "Organization":"Example Corp",
         "OrganizationalUnit":"Sales",
         "State":"WA",
         "Locality":"Seattle",
         "CommonName":"*.ec2.internal"
      }
   }
   ```

3. Simpan dan tutup file, keluar dari editor teks. Untuk informasi selengkapnya, lihat Prosedur untuk membuat CA di Panduan AWS Private Certificate Authority Pengguna.

4. Gunakan perintah AWS Private CA CLI create-certificate-authority untuk membuat CA pribadi.

   ```
   ~/home > aws acm-pca create-certificate-authority \
        --certificate-authority-configuration file://ca_config.txt \
        --certificate-authority-type "ROOT" \
        --idempotency-token 01234567 --region aws-region
   ```

   Jika berhasil, perintah ini mengeluarkan Amazon Resource Name (ARN) dari CA.

```
{
   "CertificateAuthorityArn": "arn:aws:acm-pca:aws-region:111122223333:certificate-
authority/12345678-1234-1234-1234-123456789012"
}
```

Untuk membuat dan menginstal sertifikat untuk root pribadi CA (AWS CLI)

1. Buat permintaan penandatanganan sertifikat (CSR) menggunakan perintah get-certificate-authority-csr AWS CLI.

```
$ aws acm-pca get-certificate-authority-csr \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --output text \
     --endpoint https://acm-pca.aws-region.amazonaws.com \
     --region eu-west-1 > ca.csr
```

   File yang dihasilkan `ca.csr`, file PEM yang dikodekan dalam format base64, memiliki tampilan sebagai berikut.

```
-----BEGIN CERTIFICATE-----
 MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
 VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
 b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
 BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
 MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
 VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
 b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
 YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
 21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
 rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
 Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
 nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
 FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
 NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
 -----END CERTIFICATE-----
```

   Untuk informasi selengkapnya, lihat Menginstal sertifikat CA root di Panduan AWS Private Certificate Authority Pengguna.

2. Gunakan `issue-certificate` AWS CLI perintah untuk menerbitkan dan menginstal sertifikat root pada CA pribadi Anda.

```
$ aws acm-pca issue-certificate \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --csr file://ca.csr \
     --signing-algorithm SHA256WITHRSA \
     --template-arn arn:aws:acm-pca:::template/RootCACertificate/V1 \
     --validity Value=3650,Type=DAYS --region aws-region
```

3. Unduh sertifikat root menggunakan `get-certificate` AWS CLI perintah.

```
$ aws acm-pca get-certificate \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
    --certificate-arn arn:aws:acm-pca:aws-region:486768734100:certificate-
authority/12345678-1234-1234-1234-123456789012/certificate/
abcdef0123456789abcdef0123456789 \
    --output text --region aws-region > rootCA.pem
```

4. Instal sertifikat root pada CA pribadi Anda menggunakan `import-certificate-authority-certificate` AWS CLI perintah.

```
$ aws acm-pca import-certificate-authority-certificate \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --certificate file://rootCA.pem --region aws-region
```

Menghasilkan dan mengekspor sistem file dan sertifikat klien

1. Gunakan `request-certificate` AWS CLI perintah untuk meminta AWS Certificate Manager sertifikat untuk digunakan pada sistem file dan klien Anda.

```
$ aws acm request-certificate \
    --domain-name *.ec2.internal \
    --idempotency-token 12345 \
    --region aws-region \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012
```

Jika permintaan berhasil, ARN dari sertifikat yang dikeluarkan dikembalikan.

2. Untuk keamanan, Anda harus menetapkan frasa sandi untuk kunci pribadi saat mengekspornya. Buat frasa sandi dan simpan dalam file bernama `passphrase.txt`
3. Gunakan `export-certificate` AWS CLI perintah untuk mengekspor sertifikat pribadi yang dikeluarkan sebelumnya. File yang diekspor berisi sertifikat, rantai sertifikat, dan kunci RSA 2048-bit pribadi terenkripsi yang terkait dengan kunci publik yang disematkan dalam sertifikat. Untuk keamanan, Anda harus menetapkan frasa sandi untuk kunci pribadi saat mengekspornya. Contoh berikut adalah untuk instance Linux EC2.

```
$ aws acm export-certificate \
     --certificate-arn arn:aws:acm:aws-
region:111122223333:certificate/12345678-1234-1234-1234-123456789012 \
     --passphrase $(cat passphrase.txt | base64)) --region aws-region >
 exported_cert.json
```

4. Gunakan `jq` perintah berikut untuk mengekstrak kunci pribadi dan sertifikat dari respons JSON.

```
$ cat exported_cert.json | jq -r .PrivateKey > prv.key

cat exported_cert.json | jq -r .Certificate > cert.pem
openssl rsa -in prv.key -passin pass:$passphrase -out decrypted.key
```

5. Gunakan `openssl` perintah berikut untuk mendekripsi kunci pribadi dari respons JSON. Setelah memasukkan perintah, Anda diminta untuk frasa sandi.

```
$ openssl rsa -in prv.key -passin pass:$passphrase -out decrypted.key
```

Menginstal dan mengonfigurasi Libreswan IPSec pada klien Amazon Linux 2

Bagian berikut memberikan petunjuk untuk menginstal dan mengonfigurasi Libreswan IPSec pada instans Amazon EC2 yang menjalankan Amazon Linux 2.

Untuk menginstal dan mengkonfigurasi Libreswan

1. Connect ke instans EC2 Anda menggunakan SSH. Untuk petunjuk spesifik tentang cara melakukannya, lihat Connect ke instans Linux menggunakan klien SSH di Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Linux.
2. Jalankan perintah berikut untuk menginstall`libreswan`:

```
$ sudo yum install libreswan
```

3. (Opsional) Saat memverifikasi IPsec di langkah selanjutnya, properti ini mungkin ditandai tanpa pengaturan ini. Kami menyarankan untuk menguji pengaturan Anda terlebih dahulu tanpa pengaturan ini. Jika koneksi Anda bermasalah, kembali ke langkah ini dan buat perubahan berikut.

   Setelah instalasi selesai, gunakan editor teks pilihan Anda untuk menambahkan entri berikut ke file. `/etc/sysctl.conf`

   ```
   net.ipv4.ip_forward=1
   net.ipv4.conf.all.accept_redirects = 0
   net.ipv4.conf.all.secure_redirects = 0
   net.ipv4.conf.all.send_redirects = 0
   net.ipv4.conf.default.accept_redirects = 0
   net.ipv4.conf.default.send_redirects = 0
   net.ipv4.conf.lo.accept_redirects = 0
   net.ipv4.conf.lo.send_redirects = 0
   net.ipv4.conf.all.rp_filter = 0
   net.ipv4.conf.default.rp_filter = 0
   net.ipv4.conf.eth0.rp_filter = 0
   ```

   Simpan perubahan dan keluar dari editor teks.

4. Terapkan perubahan.

   ```
   $ sudo sysctl -p
   ```

5. Verifikasi konfigurasi IPsec.

   ```
   $ sudo ipsec verify
   ```

   Verifikasi bahwa versi yang `Libreswan` Anda instal sedang berjalan.

6. Inisialisasi database IPsec NSS.

   ```
   $ sudo ipsec checknss
   ```

Untuk menginstal sertifikat pada klien

1. Salin sertifikat yang Anda buat untuk klien ke direktori kerja pada instans EC2. Anda
2. Ekspor sertifikat yang dihasilkan sebelumnya ke dalam format yang kompatibel dengan`libreswan`.

```
$ openssl pkcs12 -export -in cert.pem -inkey decrypted.key \
    -certfile rootCA.pem -out certkey.p12 -name fsx
```

3. Impor kunci yang diformat ulang, berikan frasa sandi saat diminta.

```
$ sudo ipsec import certkey.p12
```

4. Buat file konfigurasi IPsec menggunakan editor teks pilihan.

```
$ sudo cat /etc/ipsec.d/nfs.conf
```

Tambahkan entri berikut ke file konfigurasi:

```
conn fsxn
    authby=rsasig
    left=172.31.77.6
    right=198.19.254.13
    auto=start
    type=transport
    ikev2=insist
    keyexchange=ike
    ike=aes256-sha2_384;dh20
    esp=aes_gcm_c256
    leftcert=fsx
    leftrsasigkey=%cert
    leftid=%fromcert
    rightid=%fromcert
    rightrsasigkey=%cert
```

Anda akan memulai IPsec pada klien setelah mengkonfigurasi IPsec pada sistem file Anda.

Mengkonfigurasi IPsec pada sistem file Anda

Bagian ini memberikan petunjuk tentang menginstal sertifikat pada FSx Anda untuk sistem file ONTAP, dan mengkonfigurasi IPSec.

Untuk menginstal sertifikat pada sistem file Anda

1. Salin sertifikat root (`rootCA.pem`), sertifikat klien (`cert.pem`) dan file kunci (`decrypted.key`) yang didekripsi ke sistem file Anda. Anda perlu mengetahui frasa sandi untuk sertifikat.
2. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen Amazon fsX NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *`management_endpoint_ip`* dengan alamat IP port manajemen sistem file.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Untuk informasi selengkapnya, lihat Mengelola sistem file dengan ONTAP CLI.
3. Gunakan cat pada klien (bukan pada sistem file Anda) untuk daftar konten`rootCA.pem`, `cert.pem` dan `decrypted.key` file sehingga Anda dapat menyalin output dari setiap file dan menempelkannya ketika diminta dalam langkah-langkah berikut.

   ```
   $ > cat cert.pem
   ```

   Salin isi sertifikat.
4. Anda harus menginstal semua sertifikat CA yang digunakan selama autentikasi bersama, termasuk CA sisi ONTAP dan sisi klien, ke manajemen ONTAP sertifikat kecuali sudah diinstal (seperti halnya ROOT-CA yang ditandatangani sendiri ONTAP).

   Gunakan perintah `security certificate install` NetApp CLI sebagai berikut untuk menginstal sertifikat klien:

   ```
   FSxID123:: > security certificate install -vserver dr -type client -cert-name
    ipsec-client-cert
   ```

   ```
   Please enter Certificate: Press <Enter> when done
   ```

   Tempel konten `cert.pem` file yang Anda salin sebelumnya dan tekan Enter.

```
Please enter Private Key: Press <Enter> when done
```

Tempel di isi `decrypted.key` file, dan tekan enter.

```
Do you want to continue entering root and/or intermediate certificates {y|n}:
```

Masukkan n untuk menyelesaikan memasukkan sertifikat klien.

5. Buat dan instal sertifikat untuk digunakan oleh SVM. Penerbit CA sertifikat ini harus sudah diinstal ONTAP dan ditambahkan ke IPsec.

   Gunakan perintah berikut untuk menginstal sertifikat root.

```
FSxID123:: > security certificate install -vserver dr -type server-ca -cert-name
 ipsec-ca-cert
```

```
Please enter Certificate: Press <Enter> when done
```

   Tempel di isi `rootCA.pem` file, dan tekan enter.

6. Untuk memastikan bahwa CA yang diinstal berada dalam jalur pencarian CA IPsec selama otentikasi, tambahkan CA manajemen ONTAP sertifikat ke modul IPsec menggunakan perintah “security ipsec ca-certificate add”.

   Masukkan perintah berikut untuk menambahkan sertifikat root.

```
FSxID123:: > security ipsec ca-certificate add -vserver dr -ca-certs ipsec-ca-cert
```

7. Masukkan perintah berikut untuk membuat kebijakan IPsec yang diperlukan dalam database kebijakan keamanan (SPD).

```
security ipsec policy create -vserver dr -name policy-name -local-ip-
subnets 198.19.254.13/32 -remote-ip-subnets 172.31.0.0/16 -auth-method PKI -action
 ESP_TRA -cipher-suite SUITEB_GCM256 -cert-name ipsec-client-cert -local-identity
 "CN=*.ec2.internal" -remote-identity "CN=*.ec2.internal"
```

8. Gunakan perintah berikut untuk menunjukkan kebijakan IPsec untuk sistem file untuk mengonfirmasi.

```
FSxID123:: > security ipsec policy show -vserver dr -instance

                                 Vserver: dr
                             Policy Name: promise
                          Local IP Subnets: 198.19.254.13/32
                         Remote IP Subnets: 172.31.0.0/16
                               Local Ports: 0-0
                              Remote Ports: 0-0
                                 Protocols: any
                                    Action: ESP_TRA
                              Cipher Suite: SUITEB_GCM256
          IKE Security Association Lifetime: 86400
        IPsec Security Association Lifetime: 28800
IPsec Security Association Lifetime (bytes): 0
                         Is Policy Enabled: true
                            Local Identity: CN=*.ec2.internal
                           Remote Identity: CN=*.ec2.internal
                    Authentication Method: PKI
             Certificate for Local Identity: ipsec-client-cert
```

Mulai IPsec pada klien

Sekarang IPSec dikonfigurasi pada FSx untuk sistem file ONTAP dan klien, Anda dapat memulai IPSec pada klien.

1. Connect ke sistem klien Anda menggunakan SSH.
2. Mulai IPsec.

```
$ sudo ipsec start
```

3. Periksa status IPsec.

```
$ sudo ipsec status
```

4. Pasang volume pada sistem file Anda.

```
$ sudo mount -t nfs 198.19.254.13:/benchmark /home/ec2-user/acm/dr
```

5. Verifikasi pengaturan IPsec dengan menunjukkan koneksi terenkripsi pada FSx Anda untuk sistem file ONTAP.

```
FSxID123:: > security ipsec show-ikesa -node FsxId123
FsxId08ac16c7ec2781a58::> security ipsec show-ikesa -node FsxId08ac16c7ec2781a58-01
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ---------------- -----------
dr          policy-name
                   198.19.254.13   172.31.77.6     551c55de57fe8976 ESTABLISHED
fsx         policy-name
                   198.19.254.38   172.31.65.193   4fd3f22c993e60c5 ESTABLISHED
2 entries were displayed.
```

Menyiapkan IPsec untuk beberapa klien

Ketika sejumlah kecil klien perlu memanfaatkan IPSec, menggunakan entri SPD tunggal untuk setiap klien sudah cukup. Namun, ketika ratusan atau bahkan ribuan klien perlu memanfaatkan IPSec, kami sarankan Anda menggunakan beberapa konfigurasi klien IPsec.

FSx untuk ONTAP mendukung menghubungkan beberapa klien di banyak jaringan ke satu alamat IP SVM dengan IPsec diaktifkan. Anda dapat melakukannya dengan menggunakan `subnet` konfigurasi atau `Allow all clients` konfigurasi, yang dijelaskan dalam prosedur berikut:

Untuk mengkonfigurasi IPsec untuk beberapa klien menggunakan konfigurasi subnet

Untuk memungkinkan semua klien pada subnet tertentu (192.168.134.0/24 misalnya) untuk terhubung ke alamat IP SVM tunggal menggunakan entri kebijakan SPD tunggal, Anda harus menentukan dalam bentuk subnet. `remote-ip-subnets` Selain itu, Anda harus menentukan `remote-identity` bidang dengan identitas sisi klien yang benar.

> **Important**
>
> Saat menggunakan otentikasi sertifikat, setiap klien dapat menggunakan sertifikat unik mereka sendiri atau sertifikat bersama untuk mengautentikasi. FSx untuk ONTAP IPSec memeriksa validitas sertifikat berdasarkan CA yang diinstal pada toko kepercayaan lokalnya. FSx untuk ONTAP juga mendukung pemeriksaan daftar pencabutan sertifikat (CRL).

1. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen Amazon fsX NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *`management_endpoint_ip`* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat Mengelola sistem file dengan ONTAP CLI.

2. Gunakan perintah `security ipsec policy create` NetApp ONTAP CLI sebagai berikut, ganti nilai *sampel* dengan nilai spesifik Anda.

```
FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
  -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 \
  -local-ports 2049 -protocols tcp -auth-method PSK \
  -cert-name my_nfs_server_cert -local-identity ontap_side_identity \
  -remote-identity client_side_identity
```

Untuk mengkonfigurasi IPSec untuk beberapa klien menggunakan konfigurasi izinkan semua klien

Untuk mengizinkan klien mana pun, terlepas dari alamat IP sumbernya, untuk terhubung ke alamat IP berkemampuan IPsec SVM, gunakan kartu `0.0.0.0/0` liar saat menentukan bidang. `remote-ip-subnets`

Selain itu, Anda harus menentukan `remote-identity` bidang dengan identitas sisi klien yang benar. Untuk otentikasi sertifikat, Anda dapat memasukkan`ANYTHING`.

Juga, ketika kartu liar 0.0.0.0/0 digunakan, Anda harus mengonfigurasi nomor port lokal atau jarak jauh tertentu untuk digunakan. Misalnya, port NFS 2049.

1. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen Amazon fsX NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat Mengelola sistem file dengan ONTAP CLI.

2. Gunakan perintah `security ipsec policy create` NetApp ONTAP CLI sebagai berikut, ganti nilai *sampel* dengan nilai spesifik Anda.

```
FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
  -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 0.0.0.0/0 \
  -local-ports 2049 -protocols tcp -auth-method PSK \
```

```
-cert-name my_nfs_server_cert -local-identity ontap_side_identity \
-local-ports 2049 -remote-identity client_side_identity
```

Manajemen identitas dan akses untuk Amazon FSx untuk ONTAP NetApp

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diotorisasi (memiliki izin) untuk menggunakan sumber daya Amazon FSx. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Amazon FSx.

Pengguna layanan - Jika Anda menggunakan layanan Amazon FSx untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensyal dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Amazon FSx untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Amazon FSx, lihat. Memecahkan masalah Amazon FSx untuk NetApp identitas dan akses ONTAP

Administrator layanan - Jika Anda bertanggung jawab atas sumber daya Amazon FSx di perusahaan Anda, Anda mungkin memiliki akses penuh ke Amazon FSx. Tugas Anda adalah menentukan fitur dan sumber daya Amazon FSx mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Amazon FSx, lihat. Bagaimana Amazon FSx untuk NetApp ONTAP bekerja dengan IAM

Administrator IAM - Jika Anda administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Amazon FSx. Untuk melihat contoh kebijakan berbasis identitas Amazon FSx yang dapat Anda gunakan di IAM, lihat. Contoh kebijakan berbasis identitas untuk Amazon FSx untuk ONTAP NetApp

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensil yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensyal Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensyal Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani permintaan AWS API di Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-

faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) dalam AWS dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensyal sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensyal yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apakah itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci

akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin ke grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kapan harus membuat pengguna IAM (bukan peran) dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil peran IAM untuk sementara AWS Management Console dengan beralih peran. Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Menggunakan peran IAM dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama

untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.

- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Sebagai contoh, ketika Anda memanggil suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.
  - Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensyal sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan dalam instans Amazon EC2 dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat Kapan harus membuat peran IAM (bukan pengguna) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang

dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat Memilih antara kebijakan yang dikelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACL)

Daftar kontrol akses (ACL) mengendalikan prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, lihat Gambaran umum daftar kontrol akses (ACL) dalam Panduan Developer Amazon Simple Storage Service.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian

izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.

- Kebijakan kontrol layanan (SCP) — SCP adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organisasi dan SCP, lihat Cara kerja SCP dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana Amazon FSx untuk NetApp ONTAP bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Amazon FSx, pelajari fitur IAM apa yang tersedia untuk digunakan dengan Amazon FSx.

Fitur IAM yang dapat Anda gunakan dengan Amazon NetApp FSx untuk ONTAP

Fitur IAM	Dukungan Amazon FSx
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya

Fitur IAM	Dukungan Amazon FSx
Sumber daya kebijakan	Ya
Kunci kondisi kebijakan	Ya
ACL	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya
Sesi akses teruskan (FAS)	Ya
Peran layanan	Tidak
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Amazon FSx dan layanan AWS lainnya dengan sebagian besar fitur IAM, AWS lihat layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk Amazon FSx

Mendukung kebijakan berbasis identitas	Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk Amazon FSx

Untuk melihat contoh kebijakan berbasis identitas Amazon FSx, lihat. Contoh kebijakan berbasis identitas untuk Amazon FSx untuk ONTAP NetApp

Kebijakan berbasis sumber daya dalam Amazon FSx

Mendukung kebijakan berbasis sumber daya	Tidak

Tindakan kebijakan untuk Amazon FSx

Mendukung tindakan kebijakan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar tindakan Amazon FSx, lihat Tindakan yang ditentukan oleh Amazon FSx di Referensi Otorisasi Layanan.

Tindakan kebijakan di Amazon FSx menggunakan awalan berikut sebelum tindakan:

```
fsx
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [
```

```
      "fsx:action1",
      "fsx:action2"
         ]
```

Untuk melihat contoh kebijakan berbasis identitas Amazon FSx, lihat. Contoh kebijakan berbasis identitas untuk Amazon FSx untuk ONTAP NetApp

Sumber daya kebijakan untuk Amazon FSx

Mendukung sumber daya kebijakan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Untuk melihat daftar jenis sumber daya Amazon FSx dan ARNnya, lihat Sumber daya yang ditentukan oleh Amazon FSx di Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang ditentukan oleh Amazon FSx.

Untuk melihat contoh kebijakan berbasis identitas Amazon FSx, lihat. Contoh kebijakan berbasis identitas untuk Amazon FSx untuk ONTAP NetApp

Kunci kondisi kebijakan untuk Amazon FSx

Mendukung kunci kondisi kebijakan khusus layanan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi `AND` logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tag yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat Elemen kebijakan IAM: variabel dan tag dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Untuk melihat daftar kunci kondisi Amazon FSx, lihat Kunci kondisi untuk Amazon FSx di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh Amazon FSx.

Untuk melihat contoh kebijakan berbasis identitas Amazon FSx, lihat. Contoh kebijakan berbasis identitas untuk Amazon FSx untuk ONTAP NetApp

Daftar kontrol akses (ACL) di Amazon FSx

Mendukung ACL	Tidak

Kontrol akses berbasis atribut (ABAC) dengan Amazon FSx

Mendukung ABAC (tanda dalam kebijakan)	Ya

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tag milik prinsipal cocok dengan tag yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi saat manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tag di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Apa itu ABAC? dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang menandai sumber daya Amazon FSx, lihat. Memberi tanda sumber daya Amazon FSx Anda

Untuk melihat contoh kebijakan berbasis identitas untuk membatasi akses ke sumber daya berdasarkan tag pada sumber daya tersebut, lihat Menggunakan tag untuk mengontrol akses ke sumber daya Amazon FSx Anda.

Menggunakan kredensil Sementara dengan Amazon FSx

Mendukung penggunaan kredensial sementara	Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensyal sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensyal sementara, lihat Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredensyal sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensil sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Peralihan peran (konsol) dalam Panduan Pengguna IAM.

Anda dapat membuat kredensyal sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensyal sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Teruskan sesi akses untuk Amazon FSx

Mendukung sesi akses maju (FAS)	Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.

Peran layanan untuk Amazon FSx

Mendukung peran layanan	Tidak

Peran terkait layanan untuk Amazon FSx

Mendukung peran terkait layanan	Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang membuat atau mengelola peran terkait layanan Amazon FSx, lihat. Menggunakan peran terkait layanan untuk Amazon FSx

Contoh kebijakan berbasis identitas untuk Amazon FSx untuk ONTAP NetApp

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Amazon FSx. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian akan dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Amazon FSx, termasuk format ARN untuk setiap jenis sumber daya, lihat Tindakan, sumber daya, dan kunci kondisi untuk Amazon FSx di Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol Amazon FSx
- Mengizinkan pengguna melihat izin mereka sendiri

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Amazon FSx di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan.

Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan dalam IAM dalam Panduan Pengguna IAM.

Menggunakan konsol Amazon FSx

Untuk mengakses Amazon FSx untuk konsol NetApp ONTAP, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Amazon FSx di Anda. Akun AWS Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang coba mereka lakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan konsol Amazon FSx, lampirkan juga kebijakan `AmazonFSxConsoleReadOnlyAccess` AWS terkelola ke entitas. Untuk informasi selengkapnya, lihat Menambah izin untuk pengguna dalam Panduan Pengguna IAM.

Anda dapat melihat `AmazonFSxConsoleReadOnlyAccess` dan kebijakan layanan terkelola Amazon FSx lainnya di. AWS kebijakan terkelola untuk Amazon FSx

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
```

```
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Memecahkan masalah Amazon FSx untuk NetApp identitas dan akses ONTAP

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Amazon FSx dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di Amazon FSx
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Amazon FSx saya

Saya tidak berwenang untuk melakukan tindakan di Amazon FSx

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya *`my-example-widget`* rekaan, tetapi tidak memiliki izin `fsx:`*`GetWidget`* rekaan.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fsx:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya *`my-example-widget`* dengan menggunakan tindakan `fsx:`*`GetWidget`*.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan bahwa Anda tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Amazon FSx.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Amazon FSx. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Amazon FSx saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah Amazon FSx mendukung fitur-fitur ini, lihat. Bagaimana Amazon FSx untuk NetApp ONTAP bekerja dengan IAM
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara penggunaan kebijakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.

Menggunakan tag dengan Amazon FSx

Anda dapat menggunakan tag untuk mengontrol akses ke sumber daya Amazon FSx dan menerapkan kontrol akses berbasis atribut (ABAC). Untuk menerapkan tag ke sumber daya Amazon FSx selama pembuatan, pengguna harus memiliki izin AWS Identity and Access Management (IAM) tertentu.

Memberikan izin untuk memberi tanda pada sumber daya saat sumber daya tersebut dibuat

Dengan beberapa tindakan Amazon FSx API yang membuat sumber daya, Anda dapat menentukan tag saat membuat sumber daya. Anda dapat menggunakan tag sumber daya ini untuk menerapkan

kontrol akses berbasis atribut (ABAC). Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

Agar pengguna dapat menandai sumber daya pada pembuatan, mereka harus memiliki izin untuk menggunakan tindakan yang membuat sumber daya, seperti`fsx:CreateFileSystem`,`fsx:CreateStorageVirtualMachine`, atau`fsx:CreateVolume`. Jika tag ditentukan dalam tindakan pembuatan sumber daya, IAM melakukan otorisasi tambahan pada `fsx:TagResource` tindakan untuk memverifikasi apakah pengguna memiliki izin untuk membuat tag. Oleh karena itu, para pengguna juga harus memiliki izin eksplisit untuk menggunakan tindakan `fsx:TagResource`.

Contoh kebijakan berikut memungkinkan pengguna untuk membuat sistem file dan penyimpanan mesin virtual (SVM) dan menerapkan tag pada mereka selama pembuatan di tempat tertentu Akun AWS.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
         "fsx:CreateStorageVirtualMachine",
         "fsx:TagResource"
      ],
      "Resource": [
         "arn:aws:fsx:region:account-id:file-system/*",
         "arn:aws:fsx:region:account-id:file-system/*/storage-virtual-machine/*"
      ]
    }
  ]
}
```

Demikian pula, kebijakan berikut memungkinkan pengguna untuk membuat cadangan pada sistem file tertentu dan menerapkan tag apa pun ke cadangan selama pembuatan cadangan.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateBackup"
```

```
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/file-system-id*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:backup/*"
    }
  ]
}
```

`fsx:TagResource`Tindakan dievaluasi hanya jika tag diterapkan selama tindakan pembuatan sumber daya. Oleh karena itu, pengguna yang memiliki izin untuk membuat sumber daya (dengan asumsi tidak ada kondisi penandaan) tidak memerlukan izin untuk menggunakan `fsx:TagResource` tindakan jika tidak ada tag yang ditentukan dalam permintaan. Akan tetapi, jika pengguna tersebut mencoba untuk membuat sumber daya dengan tanda, maka permintaan akan gagal jika pengguna tidak memiliki izin untuk menggunakan tindakan `fsx:TagResource`.

Untuk informasi selengkapnya tentang menandai sumber daya Amazon FSx, lihat. Memberi tanda sumber daya Amazon FSx Anda Untuk informasi selengkapnya tentang penggunaan tag untuk mengontrol akses ke sumber daya Amazon FSx, lihat. Menggunakan tag untuk mengontrol akses ke sumber daya Amazon FSx Anda

Menggunakan tag untuk mengontrol akses ke sumber daya Amazon FSx Anda

Untuk mengontrol akses ke sumber daya dan tindakan Amazon FSx, Anda dapat menggunakan kebijakan IAM berdasarkan tag. Anda dapat memberikan kontrol ini dengan dua cara:

- Anda dapat mengontrol akses ke sumber daya Amazon FSx berdasarkan tag pada sumber daya tersebut.
- Anda dapat mengontrol tag mana yang dapat diteruskan dalam kondisi permintaan IAM.

Untuk informasi tentang cara menggunakan tag untuk mengontrol akses ke AWS sumber daya, lihat Mengontrol akses menggunakan tag di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang menandai sumber daya Amazon FSx saat pembuatan, lihat. Memberikan izin untuk memberi tanda pada sumber daya saat sumber daya tersebut dibuat Untuk informasi selengkapnya tentang menandai sumber daya, lihatMemberi tanda sumber daya Amazon FSx Anda.

Mengontrol akses berdasarkan tag pada sumber daya

Untuk mengontrol tindakan yang dapat dilakukan pengguna atau peran pada sumber daya Amazon FSx, Anda dapat menggunakan tag pada sumber daya. Misalnya, Anda mungkin ingin mengizinkan atau menolak operasi API tertentu pada sumber daya sistem file berdasarkan pasangan nilai kunci tag pada sumber daya.

Example Contoh kebijakan - Buat sistem file hanya ketika tag tertentu digunakan

Kebijakan ini memungkinkan pengguna untuk membuat sistem file hanya jika mereka menandainya dengan pasangan nilai kunci tag tertentu, dalam contoh ini,,`key=Department`. `value=Finance`

```
{
    "Effect": "Allow",
    "Action": [
        "fsx:CreateFileSystem",
        "fsx:TagResource"
    ],
    "Resource": "arn:aws:fsx:region:account-id:file-system/*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/Department": "Finance"
        }
    }
}
```

Example Contoh kebijakan - Buat cadangan hanya Amazon fsX untuk volume NetApp ONTAP dengan tag tertentu

Kebijakan ini memungkinkan pengguna untuk membuat backup hanya dari fsX untuk volume ONTAP yang ditandai dengan pasangan nilai kunci,. `key=Department` `value=Finance` Cadangan dibuat dengan tag`Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
```

```
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }

    ]
}
```

Example Contoh kebijakan - Buat volume dengan tag tertentu dari cadangan dengan tag tertentu

Kebijakan ini memungkinkan pengguna untuk membuat volume yang ditandai `Department=Finance` hanya dari backup yang ditandai dengan. `Department=Finance`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
```

```
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example Contoh kebijakan - Hapus sistem file dengan tag tertentu

Kebijakan ini memungkinkan pengguna untuk menghapus hanya sistem file yang diberi `Department=Finance` tag. Jika mereka membuat cadangan akhir, maka itu harus ditandai dengan`Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteFileSystem"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
```

```
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example Contoh kebijakan - Hapus volume dengan tag tertentu

Kebijakan ini memungkinkan pengguna untuk menghapus hanya volume yang ditandai. `Department=Finance` Jika mereka membuat cadangan akhir, maka itu harus ditandai dengan`Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteVolume"
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
```

```
    ]
}
```

Menggunakan peran terkait layanan untuk Amazon FSx

Amazon FSx menggunakan peran terkait layanan AWS Identity and Access Management (IAM). Peran tertaut layanan adalah jenis IAM role unik yang terkait langsung dengan Amazon FSx. Peran terkait layanan telah ditentukan sebelumnya oleh Amazon FSx dan menyertakan semua izin yang diperlukan layanan untuk memanggil layanan lain atas nama Anda. AWS

Peran tertaut layanan mempermudah pengaturan Amazon FSx karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Amazon FSx menentukan izin atas peran tertaut layanan, dan kecuali ditentukan lain, hanya Amazon FSX yang dapat menjalankan perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi sumber daya Amazon FSx karena Anda tidak dapat secara ceroboh menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran tertaut layanan, lihat Layanan yang Bekerja dengan IAM AWS dan mencari layanan yang memiliki opsi Ya di kolom Peran Tertaut Layanan. Pilih Ya bersama tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Izin peran terkait layanan untuk Amazon FSx

Amazon FSx menggunakan peran terkait layanan bernama AWSServiceRoleForAmazonFSx— Yang melakukan tindakan tertentu di akun Anda, seperti membuat Antarmuka Jaringan Elastis untuk sistem file Anda di VPC Anda, dan menerbitkan sistem file dan metrik volume. CloudWatch

Untuk pembaruan kebijakan ini, lihat AmazonF SxService RolePolicy

Detail izin

Detail izin

Izin AWSServiceRoleForAmazonFSx peran ditentukan oleh kebijakan terkelola AmazonF SxService RolePolicy AWS . Ini AWSServiceRoleForAmazonFSx memiliki izin berikut:

> **Note**
>
> AWSServiceRoleForAmazonFSx Ini digunakan oleh semua jenis sistem file Amazon FSx; beberapa izin yang terdaftar tidak berlaku untuk FSx untuk ONTAP.

- `ds`— Memungkinkan Amazon FSx untuk melihat, mengotorisasi, dan tidak mengotorisasi aplikasi di direktori Anda. AWS Directory Service
- `ec2` — Mengizinkan Amazon FSx untuk melakukan hal berikut:
  - Melihat, membuat, dan memisahkan antarmuka jaringan yang terkait dengan sistem file Amazon FSx.
  - Lihat satu atau lebih alamat IP Elastis yang terkait dengan sistem file Amazon FSx.
  - Lihat Amazon VPC, grup keamanan, dan subnet yang terkait dengan sistem file Amazon FSx.
  - Untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.
  - Buat izin bagi pengguna AWS yang berwenang untuk melakukan operasi tertentu pada antarmuka jaringan.
- `cloudwatch`— Memungkinkan Amazon FSx untuk mempublikasikan titik data metrik ke CloudWatch bawah namespace AWS/FSx.
- `route53` — Mengizinkan Amazon FSx mengasosiasikan Amazon VPC dengan zona yang dihosting privat.
- `logs`— Memungkinkan Amazon FSx untuk mendeskripsikan dan menulis ke aliran CloudWatch log Log. Ini agar pengguna dapat mengirim log audit akses file untuk sistem file FSx for Windows File Server ke CloudWatch aliran Log.
- `firehose`— Memungkinkan Amazon FSx untuk mendeskripsikan dan menulis ke aliran pengiriman Amazon Data Firehose. Ini agar pengguna dapat mempublikasikan log audit akses file untuk sistem file Amazon FSx for Windows File Server ke aliran pengiriman Amazon Data Firehose.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateFileSystem",
            "Effect": "Allow",
```

```
            "Action": [
                "ds:AuthorizeApplication",
                "ds:GetAuthorizedApplicationDetails",
                "ds:UnauthorizeApplication",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAddresses",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVPCs",
                "ec2:DisassociateAddress",
                "ec2:GetSecurityGroupsForVpc",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PutMetrics",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/FSx"
                }
            }
        },

        {
            "Sid": "TagResourceNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
```

```
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "AmazonFSx.FileSystemId"
                }
            }
        },
        {
            "Sid": "ManageNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
                }
            }
        },
        {
            "Sid": "ManageRouteTable",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
                }
            }
        },
```

```
        {
            "Sid": "PutCloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
        },
        {
            "Sid": "ManageAuditLogs",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
        }
    ]
}
```

Setiap pembaruan untuk kebijakan ini dijelaskan dalamPembaruan Amazon FSx ke AWS kebijakan terkelola.

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin Peran Tertaut Layanan di Panduan Pengguna IAM.

Membuat peran terkait layanan untuk Amazon FSx

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat sistem file di AWS Management Console, IAM CLI, atau IAM API, Amazon FSx membuat peran terkait layanan untuk Anda.

> **Important**
>
> Peran tertaut layanan ini dapat muncul di akun Anda jika Anda menyelesaikan tindakan di layanan lain yang menggunakan fitur yang disupport oleh peran ini. Untuk mempelajari lebih lanjut, lihat Peran Baru yang Muncul di Akun IAM Saya.

Jika Anda menghapus peran tertaut layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Ketika Anda membuat sistem file, Amazon FSx membuat peran tertaut layanan untuk Anda kembali.

Mengedit peran terkait layanan untuk Amazon FSx

Amazon FSx tidak mengizinkan Anda mengedit peran terkait AWSServiceRoleForAmazonFSx layanan. Setelah Anda membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi lebih lanjut, lihat Mengedit Peran Tertaut Layanan di Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Amazon FSx

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami merekomendasikan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Namun, Anda harus menghapus semua sistem file Anda sebelum Anda dapat menghapus peran tertaut layanan secara manual.

> **Note**
>
> Jika layanan Amazon FSx menggunakan peran saat Anda mencoba untuk menghapus sumber daya, maka penghapusan tersebut kemungkinan gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan konsol IAM, IAM CLI, atau IAM API untuk menghapus peran terkait layanan. AWSServiceRoleForAmazonFSx Untuk informasi lebih lanjut, lihat Menghapus Peran Tertaut Layanan di Panduan Pengguna IAM.

Wilayah yang didukung untuk peran terkait layanan Amazon FSx

Amazon FSx mensupport penggunaan peran tertaut layanan di semua wilayah tempat layanan tersedia. Untuk informasi lebih lanjut, lihat Wilayah dan Titik Akhir AWS.

AWS kebijakan terkelola untuk Amazon FSx

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat AWS kebijakan yang dikelola dalam Panduan Pengguna IAM.

AmazonF SxService RolePolicy

Memungkinkan Amazon FSx mengelola AWS sumber daya atas nama Anda. Lihat Menggunakan peran terkait layanan untuk Amazon FSx untuk mempelajari selengkapnya.

AWS kebijakan terkelola: AmazonF SxDelete ServiceLinked RoleAccess

Anda tidak dapat melampirkan `AmazonFSxDeleteServiceLinkedRoleAccess` ke entitas IAM Anda. Kebijakan ini ditautkan ke layanan dan hanya digunakan dengan peran terkait layanan untuk layanan tersebut. Anda tidak dapat melampirkan, melepaskan, memodifikasi, atau menghapus kebijakan ini. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk Amazon FSx.

Kebijakan ini memberikan izin administratif yang memungkinkan Amazon FSx menghapus Peran Tertaut Layanan untuk akses Amazon S3, yang hanya digunakan oleh Amazon FSx for Lustre.

Detail izin

Kebijakan ini mencakup izin `iam` untuk mengizinkan Amazon FSx melihat, menghapus, dan melihat status penghapusan untuk Peran Tertaut Layanan FSx untuk akses Amazon S3.

Untuk melihat izin kebijakan ini, lihat AmazonF SxDelete ServiceLinked RoleAccess di Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: AmazonF Access SxFull

Anda dapat melampirkan AmazonF SxFullAccess ke entitas IAM Anda. Kebijakan ini juga dilampirkan ke peran layanan yang mengizinkan Amazon FSx untuk melakukan tindakan atas nama Anda.

Menyediakan akses penuh ke Amazon FSx dan akses ke layanan terkait AWS .

Detail izin

Kebijakan ini mencakup izin berikut.

- `fsx`— Memungkinkan kepala sekolah akses penuh untuk melakukan semua tindakan Amazon FSx, kecuali untuk. `BypassSnaplockEnterpriseRetention`
- `ds`— Memungkinkan kepala sekolah untuk melihat informasi tentang direktori. AWS Directory Service
- `ec2`
  - Memungkinkan prinsipal untuk membuat tag di bawah kondisi yang ditentukan.
  - Untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.
- `iam` – Mengizinkan prinsipal untuk membuat layanan Amazon FSx terkait peran atas nama pengguna. Ini diperlukan agar Amazon FSx dapat mengelola AWS sumber daya atas nama pengguna.
- `logs` — Mengizinkan prinsipal untuk membuat grup log, aliran log, dan menulis peristiwa untuk aliran log. Ini diperlukan agar pengguna dapat memantau akses sistem file FSx for Windows File Server dengan mengirimkan log akses audit CloudWatch ke Log.
- `firehose`— Memungkinkan kepala sekolah untuk menulis catatan ke Amazon Data Firehose. Ini diperlukan agar pengguna dapat memantau akses sistem file FSx for Windows File Server dengan mengirimkan log akses audit ke Firehose.

Untuk melihat izin kebijakan ini, lihat AmazonF SxFull Access di Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: AmazonF SxConsole FullAccess

Anda dapat melampirkan kebijakan `AmazonFSxConsoleFullAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin administratif yang memungkinkan akses penuh ke Amazon FSx dan akses ke layanan terkait AWS melalui. AWS Management Console

Detail izin

Kebijakan ini mencakup izin berikut.

- `fsx`— Memungkinkan kepala sekolah untuk melakukan semua tindakan di konsol manajemen Amazon FSx, kecuali untuk. `BypassSnaplockEnterpriseRetention`
- `cloudwatch`— Memungkinkan kepala sekolah untuk melihat CloudWatch Alarm dan metrik di konsol manajemen Amazon FSx.
- `ds`— Memungkinkan kepala sekolah untuk daftar informasi tentang direktori. AWS Directory Service
- `ec2`
  - Memungkinkan prinsipal untuk membuat tag pada tabel rute, daftar antarmuka jaringan, tabel rute, grup keamanan, subnet dan VPC yang terkait dengan sistem file Amazon FSx.
  - Memungkinkan prinsipal untuk Untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.
- `kms`— Memungkinkan kepala sekolah untuk daftar alias untuk kunci. AWS Key Management Service
- `s3` – Mengizinkan prinsipal utama untuk mendaftar beberapa atau semua objek dalam bucket Amazon S3 (hingga 1000).
- `iam` – Memberikan izin untuk membuat peran tertaut layanan yang mengizinkan Amazon FSx melakukan tindakan atas nama pengguna.

Untuk melihat izin kebijakan ini, lihat AmazonF SxConsole FullAccess di Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: AmazonF Access SxConsole ReadOnly

Anda dapat melampirkan kebijakan `AmazonFSxConsoleReadOnlyAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin hanya-baca ke Amazon FSx dan layanan AWS terkait sehingga pengguna dapat melihat informasi tentang layanan ini di. AWS Management Console

Detail izin

Kebijakan ini mencakup izin berikut.

- `fsx` – Mengizinkan prinsipal untuk melihat informasi tentang sistem file Amazon FSx, termasuk semua tag, di Konsol Manajemen Amazon FSx.
- `cloudwatch`— Memungkinkan kepala sekolah untuk melihat CloudWatch Alarm dan metrik di Konsol Manajemen Amazon FSx.
- `ds`— Memungkinkan kepala sekolah untuk melihat informasi tentang AWS Directory Service direktori di Amazon FSx Management Console.
- `ec2`
  - Memungkinkan prinsipal untuk melihat antarmuka jaringan, grup keamanan, subnet, dan VPC yang terkait dengan sistem file Amazon FSx di Konsol Manajemen Amazon FSx.
  - Untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.
- `kms`— Memungkinkan prinsipal untuk melihat alias untuk kunci AWS Key Management Service di Konsol Manajemen Amazon FSx.
- `log`— Memungkinkan kepala sekolah untuk menggambarkan grup CloudWatch log Amazon Log yang terkait dengan akun yang membuat permintaan. Ini diperlukan agar prinsipal dapat melihat konfigurasi audit akses file yang ada untuk sistem file FSx for Windows File Server.
- `firehose`— Memungkinkan kepala sekolah untuk menjelaskan aliran pengiriman Amazon Data Firehose yang terkait dengan akun yang membuat permintaan. Ini diperlukan agar prinsipal dapat melihat konfigurasi audit akses file yang ada untuk sistem file FSx for Windows File Server.

Untuk melihat izin kebijakan ini, lihat AmazonF SxConsole ReadOnly Access di Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: AmazonF SxRead OnlyAccess

Anda dapat melampirkan kebijakan `AmazonFSxReadOnlyAccess` ke identitas IAM Anda.

Kebijakan ini mencakup izin berikut.

- `fsx` – Mengizinkan prinsipal untuk melihat informasi tentang sistem file Amazon FSx, termasuk semua tag, di Konsol Manajemen Amazon FSx.
- `ec2`— Untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.

Untuk melihat izin kebijakan ini, lihat AmazonF SxRead OnlyAccess di Panduan Referensi Kebijakan AWS Terkelola.

Pembaruan Amazon FSx ke AWS kebijakan terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Amazon FSx sejak layanan ini mulai melacak perubahan ini. Untuk pemberitahuan otomatis tentang perubahan laman ini, berlangganlah ke umpan RSS pada laman Amazon FSx Riwayat Dokumen untuk Amazon FSx untuk ONTAP NetApp .

Perubahan	Deskripsi	Tanggal
AmazonF SxService RolePolicy - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, `ec2:GetSecurityGroupsForVpc` yang memungkinkan prinsipal untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.	Januari 9, 2024
AmazonF SxRead OnlyAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, `ec2:GetSecurityGroupsForVpc` yang memungkinkan prinsipal untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.	Januari 9, 2024

Perubahan	Deskripsi	Tanggal
SxConsoleReadOnlyAkses AmazonF - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, `ec2:GetSecurityGroupsForVpc` yang memungkinkan prinsipal untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.	Januari 9, 2024
SxFullAkses AmazonF - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, `ec2:GetSecurityGroupsForVpc` yang memungkinkan prinsipal untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.	Januari 9, 2024
AmazonF SxConsole FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, `ec2:GetSecurityGroupsForVpc` yang memungkinkan prinsipal untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.	Januari 9, 2024

Perubahan	Deskripsi	Tanggal
SxFullAkses AmazonF - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan pengguna melakukan replikasi data lintas wilayah dan lintas akun untuk FSx untuk sistem file OpenZFS.	20 Desember 2023
AmazonF SxConsole FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan pengguna melakukan replikasi data lintas wilayah dan lintas akun untuk FSx untuk sistem file OpenZFS.	20 Desember 2023
SxFullAkses AmazonF - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan pengguna melakukan replikasi volume sesuai permintaan untuk FSx untuk sistem file OpenZFS.	26 November 2023
AmazonF SxConsole FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan pengguna melakukan replikasi volume sesuai permintaan untuk FSx untuk sistem file OpenZFS.	26 November 2023
SxFullAkses AmazonF - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan pengguna melihat, mengaktif kan, dan menonaktifkan dukungan VPC bersama untuk FSx untuk sistem file Multi-AZ ONTAP.	14 November 2023

Perubahan	Deskripsi	Tanggal
AmazonF SxConsole FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan pengguna melihat, mengaktif kan, dan menonaktifkan dukungan VPC bersama untuk FSx untuk sistem file Multi-AZ ONTAP.	14 November 2023
SxFullAkses AmazonF - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkin kan Amazon FSx mengelola konfigurasi jaringan untuk FSx untuk sistem file Multi-AZ OpenZFS.	9 Agustus 2023
AWS kebijakan terkelola: AmazonF SxService RolePolic y - Perbarui ke kebijakan yang ada	Amazon FSx memodifikasi `cloudwatch:PutMetr icData` izin yang ada sehingga Amazon FSx menerbitkan CloudWatch metrik ke namespace. `AWS/ FSx`	Juli 24, 2023
SxFullAkses AmazonF - Perbarui ke kebijakan yang ada	Amazon FSx memperbarui kebijakan untuk menghapus `fsx:*` izin dan menambahkan tindakan tertentu`fsx`.	13 Juli 2023
AmazonF SxConsole FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx memperbarui kebijakan untuk menghapus `fsx:*` izin dan menambahkan tindakan tertentu`fsx`.	13 Juli 2023

Perubahan	Deskripsi	Tanggal
SxConsoleReadOnlyAkses AmazonF - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkin kan pengguna melihat metrik kinerja yang ditingkatkan dan tindakan yang direkomen dasikan untuk sistem file FSx for Windows File Server di konsol Amazon FSx.	21 September 2022
AmazonF SxConsole FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkin kan pengguna melihat metrik kinerja yang ditingkatkan dan tindakan yang direkomen dasikan untuk sistem file FSx for Windows File Server di konsol Amazon FSx.	21 September 2022
AmazonF SxRead OnlyAcces s - Memulai kebijakan pelacakan	Kebijakan ini memberikan akses hanya-baca ke semua sumber daya Amazon FSx dan tag apa pun yang terkait dengannya.	4 Februari 2022
AmazonF SxDelete ServiceLi nked RoleAccess - Memulai kebijakan pelacakan	Kebijakan ini memberikan izin administratif yang memungkin kan Amazon FSx menghapus Peran Tertaut Layanan untuk akses Amazon S3.	7 Januari 2022

Perubahan	Deskripsi	Tanggal
AmazonF SxService RolePolicy - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan Amazon FSx mengelola konfigurasi jaringan untuk Amazon FSx untuk sistem file ONTAP. NetApp	2 September 2021
SxFullAkses AmazonF - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan Amazon FSx membuat tag pada tabel rute EC2 untuk panggilan down cakupan.	2 September 2021
AmazonF SxConsole FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan Amazon FSx membuat Amazon NetApp FSx untuk sistem file Multi-AZ ONTAP.	2 September 2021
AmazonF SxConsole FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan Amazon FSx membuat tag pada tabel rute EC2 untuk panggilan down cakupan.	2 September 2021

Perubahan	Deskripsi	Tanggal
AmazonF SxService RolePolicy - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan Amazon FSx mendeskripsikan dan menulis ke aliran log Log. CloudWatch Ini diperlukan agar pengguna dapat melihat log audit akses file untuk sistem file FSx for Windows File Server CloudWatch menggunakan Log.	8 Juni 2021
AmazonF SxService RolePolicy - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan Amazon FSx mendeskripsikan dan menulis ke aliran pengiriman Amazon Data Firehose. Ini diperlukan agar pengguna dapat melihat log audit akses file untuk sistem file FSx for Windows File Server menggunakan Amazon Data Firehose.	8 Juni 2021

Perubahan	Deskripsi	Tanggal
SxFullAkses AmazonF - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan prinsipal mendeskripsikan dan membuat grup log Log, aliran CloudWatch log, dan menulis peristiwa ke aliran log. Ini diperlukan agar prinsipal dapat melihat log audit akses file untuk sistem file FSx for Windows File Server menggunakan Log. CloudWatch	8 Juni 2021
SxFullAkses AmazonF - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan prinsipal mendeskripsikan dan menulis catatan ke Amazon Data Firehose. Ini diperlukan agar pengguna dapat melihat log audit akses file untuk sistem file FSx for Windows File Server menggunakan Amazon Data Firehose.	8 Juni 2021

Perubahan	Deskripsi	Tanggal
AmazonF SxConsole FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkin kan prinsipal mendeskripsikan grup log CloudWatch Amazon Logs yang terkait dengan akun yang membuat permintaan. Ini diperlukan agar prinsipal dapat memilih grup CloudWatc h log Log yang ada saat mengonfigurasi audit akses file untuk sistem file FSx for Windows File Server.	8 Juni 2021
AmazonF SxConsole FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkin kan prinsipal menjelaskan aliran pengiriman Amazon Data Firehose yang terkait dengan akun yang membuat permintaan. Ini diperlukan agar prinsipal dapat memilih aliran pengirima n Firehose yang ada saat mengonfigurasi audit akses file untuk sistem file FSx for Windows File Server.	8 Juni 2021

Perubahan	Deskripsi	Tanggal
SxConsoleReadOnlyAksesAmazonF - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan prinsipal mendeskripsikan grup log CloudWatch Amazon Logs yang terkait dengan akun yang membuat permintaan. Ini diperlukan agar prinsipal dapat melihat konfigurasi audit akses file yang ada untuk sistem file FSx for Windows File Server.	8 Juni 2021
SxConsoleReadOnlyAksesAmazonF - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan prinsipal menjelaskan aliran pengiriman Amazon Data Firehose yang terkait dengan akun yang membuat permintaan. Ini diperlukan agar prinsipal dapat melihat konfigurasi audit akses file yang ada untuk sistem file FSx for Windows File Server.	8 Juni 2021
Amazon FSx mulai melacak perubahan	Amazon FSx mulai melacak perubahan untuk kebijakan yang AWS dikelola.	8 Juni 2021

Kontrol Akses Sistem File dengan Amazon VPC

Anda mengakses Amazon FSx Anda untuk sistem file NetApp ONTAP dan SVM menggunakan nama DNS atau alamat IP dari salah satu titik akhir mereka, tergantung pada jenis aksesnya. Nama DNS

memetakan ke alamat IP pribadi dari sistem file atau elastic network interface SVM di VPC Anda. Hanya sumber daya dalam VPC terkait, atau sumber daya yang terhubung dengan VPC terkait oleh AWS Direct Connect atau VPN, yang dapat mengakses data dalam sistem file Anda melalui protokol NFS, SMB, atau iSCSI. Untuk informasi selengkapnya, lihat Apa yang dimaksud dengan Amazon VPC? dalam Panduan Pengguna Amazon VPC.

> ⚠ Warning
>
> Anda tidak harus mengubah atau menghapus antarmuka jaringan elastis yang dikaitkan dengan sistem file Anda. Memodifikasi atau menghapus antarmuka jaringan dapat menyebabkan hilangnya koneksi secara permanen antara VPC Anda dan sistem file Anda.

Grup keamanan Amazon VPC

Grup keamanan bertindak sebagai firewall virtual untuk FSx Anda untuk sistem file ONTAP untuk mengontrol lalu lintas masuk dan keluar. Aturan masuk mengontrol lalu lintas masuk ke sistem file Anda, dan aturan keluar mengontrol lalu lintas keluar dari sistem file Anda. Saat Anda membuat sistem file, Anda menentukan VPC tempat pembuatannya, dan grup keamanan default untuk VPC tersebut diterapkan. Anda dapat menambahkan aturan ke setiap grup keamanan yang memungkinkan lalu lintas ke atau dari sistem file dan SVM terkait. Anda dapat melakukan modifikasi terhadap aturan-aturan untuk grup keamanan kapan saja. Aturan baru dan yang dimodifikasi secara otomatis diterapkan ke semua sumber daya yang terkait dengan grup keamanan. Ketika Amazon FSx memutuskan apakah akan mengizinkan lalu lintas mencapai sumber daya, Amazon FSx mengevaluasi semua aturan dari semua kelompok keamanan yang terkait dengan sumber daya.

Untuk menggunakan grup keamanan untuk mengontrol akses ke sistem file Amazon FSx Anda, tambahkan aturan jalur masuk dan keluar. Aturan jalur masuk mengendalikan lalu lintas yang masuk, dan aturan jalur keluar mengendalikan lalu lintas yang keluar dari sistem file Anda. Pastikan bahwa Anda memiliki aturan lalu lintas jaringan yang tepat di grup keamanan Anda untuk memetakan Berbagi file dari sistem file Amazon FSx Anda ke sebuah folder di instans komputasi yang di-support milik Anda.

Untuk informasi selengkapnya tentang aturan grup keamanan, lihat Aturan Grup Keamanan di Panduan Pengguna Amazon EC2.

Membuat grup keamanan VPC

Untuk membuat grup keamanan untuk Amazon FSx

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2.
2. Di panel navigasi, pilih Grup Keamanan.
3. Pilih Create Security Group (Buat Grup Keamanan).
4. Tentukan nama dan deskripsi untuk grup keamanan.
5. Untuk VPC, pilih Amazon VPC yang ter-associate dengan sistem file Anda untuk membuat grup keamanan dalam VPC tersebut.
6. Untuk aturan keluar, izinkan semua lalu lintas di semua port.
7. Tambahkan aturan berikut ke port masuk grup keamanan Anda. Untuk bidang sumber, Anda harus memilih Kustom dan memasukkan grup keamanan atau rentang alamat IP yang terkait dengan instance yang perlu mengakses FSx Anda untuk sistem file ONTAP, termasuk:

   - Klien Linux, Windows, dan/atau macOS yang mengakses data dalam sistem file Anda melalui NFS, SMB, atau iSCSI.
   - Setiap sistem file/cluster ONTAP yang akan Anda peer ke sistem file Anda (misalnya, untuk menggunakan SnapMirror,, atau). SnapVault FlexCache
   - Setiap klien yang akan Anda gunakan untuk mengakses ONTAP REST API, CLI, atau ZAPIs (misalnya, instance Harvest/Grafana, Connector, atau BlueXP). NetApp NetApp

Protokol	Port	Peran
Semua ICMP	Semua	Ping instance
SSH	22	Akses SSH ke alamat IP dari manajemen cluster LIF atau manajemen node LIF
TCP	111	Panggilan prosedur jarak jauh untuk NFS
TCP	135	Panggilan prosedur jarak jauh untuk CIFS
TCP	139	Sesi layanan NetBIOS untuk CIFS
TCP	161-162	Protokol manajemen jaringan sederhana (SNMP)

Protokol	Port	Peran
TCP	443	ONTAP REST API akses ke alamat IP LIF manajemen cluster atau LIF manajemen SVM
TCP	445	Microsoft SMB/CIFS melalui TCP dengan pembingka ian NetBIOS
TCP	635	Pemasangan NFS
TCP	749	Kerberos
TCP	2049	Daemon server NFS
TCP	3260	Akses iSCSI melalui LIF data iSCSI
TCP	4045	Daemon kunci NFS
TCP	4046	Monitor status jaringan untuk NFS
TCP	10000	Protokol manajemen data jaringan (NDMP) dan komunikasi intercluster NetApp SnapMirror
TCP	11104	Manajemen komunikasi NetApp SnapMirror antar kluster
TCP	11105	SnapMirror transfer data menggunakan LIF intercluster
UDP	111	Panggilan prosedur jarak jauh untuk NFS
UDP	135	Panggilan prosedur jarak jauh untuk CIFS
UDP	137	Resolusi nama NetBIOS untuk CIFS
UDP	139	Sesi layanan NetBIOS untuk CIFS
UDP	161-162	Protokol manajemen jaringan sederhana (SNMP)
UDP	635	Pemasangan NFS
UDP	2049	Daemon server NFS

Protokol	Port	Peran
UDP	4045	Daemon kunci NFS
UDP	4046	Monitor status jaringan untuk NFS
UDP	4049	Protokol kuota NFS

8. Tambahkan grup keamanan ke elastic network interface sistem file.

Larang akses ke sistem file

Untuk sementara melarang akses jaringan ke sistem file Anda dari semua klien, Anda dapat menghapus semua grup keamanan yang dikaitkan dengan antarmuka jaringan elastis dari sistem file Anda dan menggantinya dengan grup yang tidak memiliki aturan jalur masuk/jalur keluar.

Validasi Kepatuhan untuk Amazon NetApp FSx untuk ONTAP

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.
- Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

> **Note**
>
> Tidak semua memenuhi Layanan AWS syarat HIPAA. Untuk informasi selengkapnya, lihat Referensi Layanan yang Memenuhi Syarat HIPAA.

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Amazon fsX untuk NetApp ONTAP dan titik akhir VPC antarmuka ()AWS PrivateLink

Anda dapat meningkatkan postur keamanan VPC Anda dengan mengonfigurasi Amazon FSx untuk menggunakan titik akhir VPC antarmuka. Endpoint VPC antarmuka didukung oleh AWS PrivateLink,

teknologi yang memungkinkan Anda mengakses Amazon fsX API secara pribadi tanpa gateway internet, perangkat NAT, koneksi VPN, atau koneksi. AWS Direct Connect Instans di VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi dengan Amazon fsX API. Lalu lintas antara VPC Anda dan Amazon FSx tidak meninggalkan jaringan. AWS

Setiap antarmuka VPC endpoint diwakili oleh satu atau lebih antarmuka jaringan elastis di subnet Anda. Antarmuka jaringan menyediakan alamat IP pribadi yang berfungsi sebagai titik masuk untuk lalu lintas ke Amazon FSx API.

Pertimbangan untuk titik akhir VPC antarmuka Amazon FSx

Sebelum Anda menyiapkan titik akhir VPC antarmuka untuk Amazon fsX, pastikan untuk meninjau properti dan batasan titik akhir VPC Antarmuka di Panduan Pengguna Amazon VPC.

Anda dapat memanggil salah satu operasi Amazon FSx API dari VPC Anda. Misalnya, Anda dapat membuat fsX untuk sistem file ONTAP dengan memanggil CreateFileSystem API dari dalam VPC Anda. Untuk daftar lengkap API Amazon FSx, lihat Tindakan di Referensi API Amazon FSx.

Pertimbangan mengintip VPC

Anda dapat menghubungkan VPC lain ke VPC dengan titik akhir VPC antarmuka menggunakan VPC peering. Peering VPC adalah koneksi jaringan di antara dua VPC. Anda dapat membuat koneksi peering VPC antara dua VPC Anda sendiri, atau dengan VPC di VPC lain. Akun AWS VPC juga bisa dalam dua yang berbeda Wilayah AWS.

Lalu lintas antara VPC peered tetap berada di AWS jaringan dan tidak melintasi internet publik. Setelah VPC dipeer, sumber daya seperti Amazon Elastic Compute Cloud (Amazon EC2) instans di kedua VPC dapat mengakses Amazon fsX API melalui titik akhir VPC antarmuka yang dibuat di salah satu VPC.

Membuat titik akhir VPC antarmuka untuk Amazon FSx API

Anda dapat membuat titik akhir VPC untuk Amazon FSx API menggunakan konsol VPC Amazon atau (). AWS Command Line Interface AWS CLI Untuk informasi selengkapnya, lihat Membuat titik akhir VPC antarmuka di Panduan Pengguna Amazon VPC.

Untuk membuat titik akhir VPC antarmuka untuk Amazon FSx, gunakan salah satu dari berikut ini:

- **`com.amazonaws.`*`region`*`.fsx`**— Membuat titik akhir untuk operasi Amazon FSx API.

- **`com.amazonaws.`*`region`*`.fsx-fips`**— Membuat titik akhir untuk Amazon FSx API yang sesuai dengan Federal Information Processing Standard (FIPS) 140-2.

Untuk menggunakan opsi DNS pribadi, Anda harus mengatur `enableDnsHostnames` dan `enableDnsSupport` atribut VPC Anda. Untuk informasi selengkapnya, lihat Melihat dan memperbarui dukungan DNS untuk VPC Anda di Panduan Pengguna Amazon VPC.

Tidak termasuk Wilayah AWS di China, jika Anda mengaktifkan DNS pribadi untuk titik akhir, Anda dapat membuat permintaan API ke Amazon fsX dengan titik akhir VPC menggunakan nama DNS default untuk, misalnya. Wilayah AWS`fsx.us-east-1.amazonaws.com` Untuk China (Beijing) dan China (Ningxia) Wilayah AWS, Anda dapat membuat permintaan API dengan titik akhir VPC `fsx-api.cn-north-1.amazonaws.com.cn` menggunakan `fsx-api.cn-northwest-1.amazonaws.com.cn` dan, masing-masing.

Untuk informasi selengkapnya, lihat Mengakses layanan melalui titik akhir VPC antarmuka di Panduan Pengguna Amazon VPC.

Membuat kebijakan titik akhir VPC untuk Amazon FSx

Untuk mengontrol akses ke Amazon FSx API, Anda dapat melampirkan kebijakan AWS Identity and Access Management (IAM) ke titik akhir VPC Anda. Kebijakan menentukan informasi berikut:

- Prinsipal yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan.
- Sumber daya yang menjadi target tindakan.

Untuk informasi selengkapnya, lihat Mengontrol Akses ke Layanan dengan titik akhir VPC dalam Panduan Pengguna Amazon VPC.

Ketahanan di Amazon FSx untuk ONTAP NetApp

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan

memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur AWS Global.

Selain infrastruktur AWS global, Amazon FSx menawarkan beberapa fitur untuk membantu mendukung ketahanan data dan kebutuhan cadangan Anda.

Pencadangan dan pemulihan

Amazon FSx membuat dan menyimpan backup otomatis volume di Amazon fsX Anda untuk sistem file ONTAP. NetApp Amazon FSx membuat cadangan otomatis volume Anda selama jendela cadangan Amazon fsX Anda untuk sistem file ONTAP. NetApp Amazon FSx menyimpan cadangan otomatis volume Anda sesuai dengan periode retensi cadangan yang Anda tentukan. Anda juga dapat mencadangkan volume Anda secara manual, dengan membuat cadangan yang diprakarsai pengguna. Anda mengembalikan cadangan volume kapan saja dengan membuat volume baru dengan cadangan yang ditentukan sebagai sumbernya.

Untuk informasi selengkapnya, lihat Menggunakan cadangan.

Snapshot

Amazon FSx membuat salinan snapshot dari Amazon FSx untuk volume ONTAP. NetApp Salinan snapshot menawarkan perlindungan terhadap penghapusan atau modifikasi file yang tidak disengaja dalam volume Anda oleh pengguna akhir. Untuk informasi selengkapnya, lihat Cara menggunakan snapshot.

Zona Ketersediaan

Amazon FSx untuk sistem file NetApp ONTAP dirancang untuk menyediakan ketersediaan data yang berkelanjutan bahkan jika server gagal. Setiap sistem file didukung oleh dua server file di setidaknya satu Availability Zone, masing-masing dengan penyimpanannya sendiri. Amazon FSx secara otomatis mereplikasi data Anda untuk melindunginya dari kegagalan komponen, terus memantau kegagalan perangkat keras, dan secara otomatis mengganti komponen infrastruktur jika terjadi kegagalan. Sistem file secara otomatis gagal berulang-ulang sesuai kebutuhan (biasanya dalam 60 detik), dan klien secara otomatis gagal berulang-ulang dengan sistem file.

Sistem file multi-AZ

Amazon FSx untuk sistem file NetApp ONTAP sangat tersedia dan tahan lama di seluruh AWS Availability Zone, dan dirancang untuk menyediakan ketersediaan data yang berkelanjutan bahkan jika Availability Zone tidak tersedia.

Untuk informasi selengkapnya, lihat Ketersediaan dan daya tahan.

Sistem file single-AZ

Amazon FSx untuk sistem file NetApp ONTAP sangat tersedia dan tahan lama dalam satu AWS Availability Zone, dan dirancang untuk menyediakan ketersediaan berkelanjutan dalam Availability Zone tersebut jika terjadi server file individual atau kegagalan disk.

Untuk informasi selengkapnya, lihat Ketersediaan dan daya tahan.

Keamanan infrastruktur di Amazon FSx untuk ONTAP NetApp

Sebagai layanan terkelola, Amazon FSx untuk NetApp ONTAP dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Amazon FSx melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal IAM. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

Gunakan NetApp ONTAP Vscan dengan fsX untuk ONTAP

Anda dapat menggunakan fitur Vscan NetApp ONTAP untuk menjalankan perangkat lunak antivirus pihak ketiga yang didukung. Untuk informasi selengkapnya, lihat sumber daya berikut untuk setiap solusi yang didukung.

- McAfee — Panduan Solusi Antivirus untuk Data Clustered ONTAP: McAfee
- SentinelOne — Solusi mitra Vscan dan SentinelOne Singularity Cloud Data Security
- Symantec - Solusi mitra Vscan dan Mesin Perlindungan Symantec
- Trend Micro — Panduan Solusi Antivirus untuk Data Berkelompok ONTAP: Trend Micro

Peran dan pengguna di Amazon FSx untuk ONTAP NetApp

NetApp ONTAPmencakup kemampuan kontrol akses berbasis peran (RBAC) yang kuat dan dapat diperluas. ONTAPperan menentukan kemampuan dan hak istimewa pengguna saat menggunakan ONTAP CLI dan REST API. Setiap peran mendefinisikan tingkat kemampuan administratif dan hak istimewa yang berbeda. Anda menetapkan peran kepada pengguna untuk tujuan mengontrol akses mereka ke FSx untuk sumber daya ONTAP saat menggunakan REST API dan ONTAP CLI. Ada ONTAP peran yang tersedia secara terpisah untuk FSx untuk pengguna sistem file ONTAP dan pengguna mesin virtual penyimpanan (SVM).

Saat Anda membuat FSx untuk sistem file ONTAP, ONTAP pengguna default dibuat di tingkat sistem file dan di tingkat SVM. Anda dapat membuat sistem file tambahan dan pengguna SVM, dan Anda dapat membuat peran SVM tambahan untuk memenuhi kebutuhan organisasi Anda. Bab ini menjelaskan ONTAP pengguna dan peran, dan menyediakan prosedur terperinci untuk membuat pengguna tambahan dan peran SVM.

Peran administrator sistem file dan pengguna

Pengguna sistem ONTAP file default adalah`fsxadmin`, yang memiliki `fsxadmin` peran yang ditetapkan untuk itu. Ada dua peran standar yang dapat Anda tetapkan untuk pengguna sistem file, yang tercantum sebagai berikut:

- **`fsxadmin`**—Administrator dengan peran ini memiliki hak yang tidak terbatas dalam sistem. ONTAP Mereka dapat mengkonfigurasi semua sistem file dan sumber daya tingkat SVM yang tersedia di FSx untuk sistem file ONTAP.

- **`fsxadmin-readonly`**—Administrator dengan peran ini dapat melihat semuanya di tingkat sistem file tetapi tidak dapat membuat perubahan apa pun.

  Peran ini sangat cocok untuk digunakan dengan aplikasi pemantauan seperti NetApp Harvest karena memiliki akses hanya-baca ke semua sumber daya yang tersedia dan propertinya, tetapi tidak dapat membuat perubahan apa pun padanya.

Anda dapat membuat pengguna sistem file tambahan dan menetapkan mereka baik `fsxadmin-readonly` peran `fsxadmin` atau. Anda tidak dapat membuat peran baru atau memodifikasi peran yang ada. Untuk informasi selengkapnya, lihat Membuat ONTAP pengguna baru untuk sistem file dan administrasi SVM.

Tabel berikut menjelaskan tingkat akses yang dimiliki peran administrator sistem file untuk perintah ONTAP CLI dan REST API dan direktori perintah.

Nama peran	Tingkat akses	Untuk perintah atau direktori perintah berikut
`fsxadmin`	all	Semua direktori perintah tersedia di fsX untuk ONTAP
`fsxadmin-readonly`	all	`security login password` Untuk mengelola akun pengguna sendiri kata sandi lokal dan informasi kunci saja
	none	`security`
	hanya-baca	Semua direktori perintah lainnya tersedia di fsX untuk ONTAP

Peran administrator SVM dan pengguna

Setiap SVM memiliki domain otentikasi terpisah dan dapat dikelola secara independen oleh administratornya sendiri. Untuk setiap SVM di sistem file Anda, pengguna default adalah vsadmin,

yang memiliki `vsadmin` peran yang ditetapkan secara default. Selain `vsadmin` peran, ada peran SVM standar lainnya yang memberikan izin cakupan bawah yang dapat Anda tetapkan ke pengguna SVM. Anda juga dapat membuat peran khusus yang menyediakan tingkat kontrol akses yang memenuhi kebutuhan organisasi Anda.

Peran yang telah ditentukan untuk administrator SVM dan kemampuannya adalah sebagai berikut:

Nama peran	Kemampuan
`vsadmin`	• Mengelola akun pengguna Anda, kata sandi lokal, dan informasi kunci • Kelola volume, kecuali untuk pergerakan volume • Kelola kuota, qtrees, salinan Snapshot, dan file • Kelola LUN • Lakukan SnapLock operasi, kecuali untuk penghapusan hak istimewa • Konfigurasikan protokol: NFS, SMB, dan iSCSI • Konfigurasi layanan: DNS, LDAP, dan NIS • Pantau pekerjaan • Pantau koneksi jaringan dan antarmuka jaringan • Pantau kesehatan SVM
`vsadmin-volume`	• Mengelola akun pengguna Anda, kata sandi lokal, dan informasi kunci • Kelola volume, termasuk pergerakan volume • Kelola kuota, qtrees, salinan Snapshot, dan file • Kelola LUN • Konfigurasikan protokol: NFS, SMB, dan iSCSI • Konfigurasi layanan: DNS, LDAP, dan NIS

Nama peran	Kemampuan
	• Pantau antarmuka jaringan • Pantau kesehatan SVM
`vsadmin-protocol`	• Mengelola akun pengguna Anda, kata sandi lokal, dan informasi kunci • Kelola LUN • Konfigurasikan protokol: NFS, SMB, dan iSCSI • Konfigurasi layanan: DNS, LDAP, dan NIS • Monitor antarmuka jaringan • Pantau kesehatan SVM
`vsadmin-backup`	• Mengelola akun pengguna Anda, kata sandi lokal, dan informasi kunci • Kelola operasi NDMP • Buat volume baca/tulis yang dipulihkan • Mengelola SnapMirror hubungan dan salinan Snapshot • Lihat volume dan informasi jaringan

Nama peran	Kemampuan
`vsadmin-snaplock`	• Mengelola akun pengguna Anda, kata sandi lokal, dan informasi kunci • Kelola volume, kecuali untuk pergerakan volume • Kelola kuota, qtrees, salinan Snapshot, dan file • Lakukan SnapLock operasi, termasuk penghapusan hak istimewa • Konfigurasikan protokol: NFS dan SMB • Konfigurasi layanan: DNS, LDAP, dan NIS • Pantau pekerjaan • Pantau koneksi jaringan dan antarmuka jaringan
`vsadmin-readonly`	• Mengelola akun pengguna Anda, kata sandi lokal, dan informasi kunci • Pantau kesehatan SVM • Pantau antarmuka jaringan • Lihat volume dan LUNs • Lihat layanan dan protokol

Untuk informasi selengkapnya tentang cara membuat peran SVM baru, lihatMembuat peran SVM baru.

Menggunakan Active Directory untuk mengautentikasi pengguna ONTAP

Anda dapat mengautentikasi akses pengguna domain Windows Active Directory ke FSx untuk sistem file ONTAP dan SVM. Anda harus melakukan tugas-tugas berikut sebelum akun Active Directory dapat mengakses sistem file Anda:

- Anda perlu mengkonfigurasi akses pengontrol domain Active Directory ke SVM.

SVM yang Anda gunakan untuk mengonfigurasi sebagai gateway atau terowongan untuk akses pengontrol domain Active Directory harus mengaktifkan CIFS, digabungkan ke Active Directory, atau keduanya. Jika Anda tidak mengaktifkan CIFS dan hanya bergabung dengan terowongan SVM ke Active Directory, pastikan SVM bergabung dengan Active Directory Anda. Untuk informasi selengkapnya, lihat Bergabung dengan SVM ke Microsoft Active Directory.

- Anda perlu mengaktifkan akun pengguna domain Active Directory untuk mengakses sistem file.

  Anda dapat menggunakan otentikasi kata sandi atau otentikasi kunci publik SSH untuk pengguna domain Windows yang mengakses ONTAP CLI atau REST API.

Untuk prosedur yang menjelaskan cara menggunakan untuk mengonfigurasi otentikasi Active Directory untuk sistem file dan administrator SVM, lihat. Mengkonfigurasi otentikasi Active Directory untuk pengguna ONTAP

Membuat ONTAP pengguna baru untuk sistem file dan administrasi SVM

Setiap ONTAP pengguna dikaitkan dengan SVM atau sistem file. Pengguna sistem file dengan `fsxadmin` peran dapat membuat peran dan pengguna SVM baru dengan menggunakan perintah `security login create`ONTAPCLI.

`security login create`Perintah membuat metode login untuk utilitas manajemen. Metode login terdiri dari nama pengguna, aplikasi (metode akses), dan metode otentikasi. Nama pengguna dapat dikaitkan dengan beberapa aplikasi. Secara opsional dapat menyertakan nama peran kontrol akses. Jika nama grup Active Directory, LDAP, atau NIS digunakan, maka metode login memberikan akses ke pengguna yang termasuk dalam grup yang ditentukan. Jika pengguna adalah anggota dari beberapa grup yang disediakan dalam tabel login keamanan, maka pengguna akan mendapatkan akses ke daftar gabungan perintah yang diotorisasi untuk masing-masing grup.

Untuk informasi yang menjelaskan cara membuat ONTAP pengguna baru, lihatMembuat pengguna ONTAP baru.

Topik

- Membuat pengguna ONTAP baru
- Membuat peran SVM baru
- Mengkonfigurasi otentikasi Active Directory untuk pengguna ONTAP
- Mengkonfigurasi otentikasi kunci publik

- Memperbarui persyaratan kata sandi untuk sistem file dan peran SVM
- Gagal memperbarui kata sandi fsxadmin akun

Membuat pengguna ONTAP baru

Untuk membuat SVM baru atau pengguna sistem file (ONTAPCLI)

Hanya pengguna sistem file dengan `fsxadmin` peran yang dapat membuat SVM baru dan pengguna sistem file.

1. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen Amazon fsX NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *`management_endpoint_ip`* dengan alamat IP port manajemen sistem file.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Untuk informasi selengkapnya, lihat Mengelola sistem file dengan ONTAP CLI.
2. Gunakan perintah `security login create` ONTAP CLI untuk membuat akun pengguna baru di FSx Anda untuk sistem file ONTAP atau SVM.

   Masukkan data Anda untuk placeholder dalam contoh untuk menentukan properti wajib berikut:

   - `-vserver`— Menentukan nama SVM di mana Anda ingin membuat peran SVM baru atau pengguna. Jika Anda membuat peran sistem file atau pengguna, jangan tentukan SVM.
   - `-user-or-group-name`- Menentukan nama pengguna atau nama grup Active Directory dari metode login. Nama grup Active Directory hanya dapat ditentukan dengan metode `domain` otentikasi dan `ssh` aplikasi `ontapi` dan.
   - `-application`- Menentukan penerapan metode login. Nilai yang mungkin termasuk http, ontapi, dan ssh.
   - `-authentication-method`- Menentukan metode otentikasi untuk login. Kemungkinan nilainya mencakup berikut ini:
     - domain — Gunakan untuk otentikasi Active Directory
     - kata sandi - Gunakan untuk otentikasi kata sandi
     - publickey — Pengguna untuk otentikasi kunci publik
   - `-role`- Menentukan nama peran akses-kontrol untuk metode login. Pada tingkat sistem file, satu-satunya peran yang dapat ditentukan adalah. `fsxadmin`

(Opsional) Anda juga dapat menggunakan satu atau lebih parameter berikut dengan perintah:

- `[-comment]`— Gunakan untuk menyertakan notasi atau komentar untuk akun pengguna. Misalnya, **`Guest account`**. Panjang maksimum adalah 128 karakter.
- `[-second-authentication-method {none|publickey|password|nsswitch}]`- Menentukan metode otentikasi faktor kedua. Anda dapat menentukan metode berikut:
  - kata sandi - Gunakan untuk otentikasi kata sandi
  - publickey — Gunakan untuk otentikasi Public-key
  - nsswitch - Gunakan untuk otentikasi NIS atau LDAP
  - none - Nilai default jika Anda tidak menentukan satu

```
Fsx0123456::> security login create -vserver vserver_name -user-or-group-
name user_or_group_name -application login_application -authentication-
method auth_method -role role_or_account_name
```

Perintah berikut membuat pengguna sistem file baru `new_fsxadmin` dengan `fsxadmin-readonly` peran yang ditetapkan, menggunakan SSH dengan kata sandi untuk masuk. Saat diminta, berikan kata sandi untuk pengguna.

```
Fsx0123456::> security login create -user-or-group-name new_fsxadmin -application
 ssh -authentication-method password -role fsxadmin-readonly

Please enter a password for user 'new_fsxadmin':
Please enter it again:

Fsx0123456::>
```

3. Perintah berikut membuat pengguna SVM baru `new_vsadmin` di `fsx` SVM dengan `vsadmin_readonly` peran, dikonfigurasi untuk menggunakan SSH dengan kata sandi untuk masuk. Saat diminta, berikan kata sandi untuk pengguna.

```
Fsx0123456::> security login create -vserver fsx  -user-or-group-name new_vsadmin -
application ssh -authentication-method password -role vsadmin-readonly

Please enter a password for user 'new_vsadmin':
Please enter it again:
```

```
Fsx0123456::>
```

4. Perintah berikut membuat pengguna sistem file read-only baru `harvest2-user` yang akan digunakan oleh aplikasi NetApp Harvest untuk mengumpulkan metrik kinerja dan kapasitas. Untuk informasi selengkapnya, lihat Memantau FSx untuk sistem file ONTAP menggunakan Harvest dan Grafana.

```
Fsx0123456::> security login create -user-or-group-name harvest2-user -application
 ssh -role fsxadmin-readonly -authentication-method password
```

Untuk melihat informasi untuk semua sistem file dan pengguna SVM

- Gunakan perintah berikut untuk melihat semua informasi login untuk sistem file dan SVM Anda.

```
Fsx0123456::> security login show

Vserver: Fsx0123456
                                                                 Second
User/Group                Authentication                 Acct    Authentication
Name           Application Method        Role Name        Locked  Method
-------------- ----------- ------------- ---------------- ------ --------------
autosupport    console     password      autosupport      no     none
fsxadmin       http        password      fsxadmin         no     none
fsxadmin       ontapi      password      fsxadmin         no     none
fsxadmin       ssh         password      fsxadmin         no     none
fsxadmin       ssh         publickey     fsxadmin         -      none
new_fsxadmin   ssh         password      fsxadmin-readonly
                                                        no     none

Vserver: fsx
                                                                 Second
User/Group                Authentication                 Acct    Authentication
Name           Application Method        Role Name        Locked  Method
-------------- ----------- ------------- ---------------- ------ --------------
new_vsadmin    ssh         password      vsadmin-readonly no     none
vsadmin        http        password      vsadmin          yes    none
vsadmin        ontapi      password      vsadmin          yes    none
vsadmin        ssh         password      vsadmin          yes    none
10 entries were displayed.
```

```
Fsx0123456::>
```

Membuat peran SVM baru

Setiap SVM yang Anda buat memiliki administrator SVM default yang menetapkan peran yang telah ditentukan sebelumnya`vsadmin`. Selain set peran SVM yang telah ditentukan, Anda dapat membuat peran SVM baru. Jika Anda perlu membuat peran baru untuk SVM Anda, gunakan perintah `security login role create` ONTAP CLI. Perintah ini tersedia untuk administrator sistem file dengan `fsxadmin` peran.

Untuk membuat peran SVM baru (ONTAP CLI)

1. Anda dapat membuat peran SVM baru menggunakan `security login role create` ONTAP CLI perintah:

   ```
   Fsx0123456::> security login role create -role vol_role -cmddirname volume
   ```

2. Tentukan parameter yang diperlukan berikut dalam perintah:

   - `-role`- Nama peran.
   - `-cmddirname`— Direktori perintah atau perintah tempat peran memberikan akses. Lampirkan nama subdirektori perintah dalam tanda kutip ganda. Misalnya, `"volume snapshot"`. Masukkan `DEFAULT` untuk menentukan semua direktori perintah.

3. (Opsional) Anda juga dapat menambahkan salah satu parameter berikut ke perintah:

   - `-vserver`— Nama SVM yang terkait dengan peran tersebut.
   - `-access`— Tingkat akses untuk peran tersebut. Untuk direktori perintah, ini termasuk:
     - none— Menolak akses ke perintah di direktori perintah. Ini adalah nilai default untuk peran kustom.
     - `readonly`— Memberikan akses ke perintah show di direktori perintah dan subdirektorinya.
     - `all`— Memberikan akses ke semua perintah di direktori perintah dan subdirektorinya. Untuk memberikan atau menolak akses ke perintah intrinsik, Anda harus menentukan direktori perintah.

     Untuk perintah non-intrinsik (perintah yang tidak diakhiri dengan`create`,, `modify``delete`, atau): `show`

- none— Menolak akses ke perintah di direktori perintah. Ini adalah nilai default untuk peran kustom.
- readonly- Tidak berlaku. Jangan gunakan.
- all— Memberikan akses ke perintah.

- -query— Objek query yang digunakan untuk memfilter tingkat akses, yang ditentukan dalam bentuk opsi yang valid untuk perintah, atau untuk perintah di direktori perintah. Lampirkan objek kueri dalam tanda kutip ganda.

4. Jalankan perintah security login role create.

   Perintah berikut membuat peran kontrol akses bernama “admin” untuk vs1.example.com Vserver. Peran memiliki semua akses ke perintah “volume” tetapi hanya dalam agregat “aggr0".

```
Fsx0123456::>security login role create -role admin -cmddirname volume -query "-
aggr aggr0" -access all -vserver vs1.example.com
```

Mengkonfigurasi otentikasi Active Directory untuk pengguna ONTAP

Gunakan ONTAP CLI untuk mengonfigurasi penggunaan otentikasi Active Directory untuk sistem ONTAP file dan pengguna SVM.

Anda harus menjadi administrator sistem file dengan fsxadmin peran untuk menggunakan perintah dalam prosedur ini.

Untuk mengatur otentikasi Active Directory untuk ONTAP pengguna (ONTAPCLI)

Perintah dalam prosedur ini tersedia untuk pengguna sistem file dengan fsxadmin peran tersebut.

1. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen Amazon fsX NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

   Untuk informasi selengkapnya, lihat Mengelola sistem file dengan ONTAP CLI.

2. Gunakan security login domain-tunnel createperintah seperti yang ditunjukkan untuk membuat terowongan domain untuk mengautentikasi pengguna Windows Active Directory. Ganti *svm_name* dengan nama SVM yang Anda gunakan untuk terowongan domain.

```
FsxId0123456::> security login domain-tunnel create -vserver svm_name
```

3. Gunakan `security login create`perintah untuk membuat akun pengguna domain Active Directory yang akan mengakses sistem file.

   Tentukan parameter yang diperlukan berikut dalam perintah:

   - `-vserver`— Nama SVM dikonfigurasi dengan CIFS dan bergabung dengan Active Directory Anda. Ini akan digunakan sebagai terowongan untuk mengautentikasi pengguna domain Active Directory ke sistem file. yang peran atau pengguna baru akan dibuat.
   - `-user-or-group-name`— Nama pengguna atau nama grup Direktori Aktif dari metode login. Nama grup Active Directory hanya dapat ditentukan dengan metode `domain` otentikasi dan `ontapi` dan `ssh` aplikasi.
   - `-application`— Penerapan metode login. Nilai yang mungkin termasuk http, ontapi, dan ssh.
   - `-authentication-method`— Metode otentikasi yang digunakan untuk login. Kemungkinan nilainya mencakup berikut ini:
     - domain — untuk otentikasi Active Directory
     - kata sandi - untuk otentikasi kata sandi
     - publickey — untuk otentikasi kunci publik
   - `-role`— Nama peran kontrol akses untuk metode login. Pada tingkat sistem file, satu-satunya peran yang dapat ditentukan adalah. `-role fsxadmin`

   Contoh berikut membuat akun pengguna domain Active Directory `CORP\Admin` untuk sistem `filesystem1` file.

```
FSxId012345::> security login create -vserver filesystem1 -username CORP\Admin -
application ssh -authmethod domain -role fsxadmin
```

   Contoh berikut membuat akun `CORP\Admin` pengguna dengan otentikasi kunci publik.

```
FsxId0123456ab::> security login create -user-or-group-name "CORP\Admin" -
application ssh -authentication-method publickey -role fsxadmin
Warning: To use public-key authentication, you must create a public key for user
 "CORP\Admin".
```

Buat kunci publik untuk `CORP\Admin` pengguna menggunakan perintah berikut:

```
FsxId0123456ab::> security login publickey create -username "CORP
\Admin" -publickey "ecdsa-sha2-nistp256 SECRET_STRING_HERE_IS_REDACTED=
 cwaltham@b0be837a91bf.ant.amazon.com"
```

Untuk masuk ke sistem file menggunakan SSH dengan kredensyal Active Directory

- Contoh berikut menunjukkan bagaimana SSH ke dalam sistem file Anda dengan kredensi Active Directory Anda jika Anda memilih `ssh` untuk jenis. `-application` Ada `username` dalam format`"domain-name\user-name"`, yang merupakan nama domain dan nama pengguna yang Anda berikan saat membuat akun, dipisahkan oleh garis miring terbalik dan dilampirkan dalam kutipan.

  ```
  Fsx0123456::> ssh "CORP\user"@management.fs-abcdef01234567892.fsx.us-east-2.aws.com
  ```

  Saat diminta memasukkan kata sandi, gunakan kata sandi pengguna Active Directory.

Mengkonfigurasi otentikasi kunci publik

Untuk mengaktifkan otentikasi kunci publik SSH, Anda harus terlebih dahulu membuat kunci SSH dan mengaitkannya dengan akun administrator dengan menggunakan perintah. `security login publickey create` Ini memungkinkan akun untuk mengakses SVM. `security login publickey create`Perintah menerima parameter berikut.

Parameter	Deskripsi
`-vserver` (Opsional)	Nama SVM yang diakses akun. Jika Anda mengonfigurasi otentikasi kunci publik SSH untuk pengguna sistem file, jangan sertakan. `-versver`
`-username`	Nama pengguna akun. Nilai default,`admin`, adalah nama default administrator cluster.

Parameter	Deskripsi
`-index`	Nomor indeks kunci publik. Nilai default adalah 0 jika kunci adalah kunci pertama yang dibuat untuk akun. Jika tidak, nilai default adalah satu lebih dari nomor indeks tertinggi yang ada untuk akun.
`-publickey`	Kunci publik OpenSSH. Lampirkan kunci dalam tanda kutip ganda.
`-role`	Peran kontrol akses yang ditetapkan ke akun.
`-comment` (Opsional)	Teks deskriptif untuk kunci publik. Lampirkan teks dalam tanda kutip ganda.

Contoh berikut mengaitkan kunci publik dengan akun administrator SVM `svmadmin` untuk SVM. `svm01` Kunci publik diberi nomor indeks`5`.

```
Fsx0123456::> security login publickey create -vserver svm01 -username svmadmin
 -index 5 -publickey "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAspH64CYbUsDQCdW22JnK6J/
vU9upnKzd2zAk9C1f7YaWRUAFNs2Qe5lUmQ3ldi8AD0Vfbr5T6HZPCixNAIzaFciDy7hgnmdj9eNGedGr/
JNrftQbLD1hZybX
+72DpQB0tYWBhe6eDJ1oPLobZBGfMlPXh8VjeU44i7W4+s0hG0E=tsmith@publickey.example.com"
```

> **Important**
>
> Anda harus menjadi SVM atau administrator sistem file untuk melakukan tugas ini.

Memperbarui persyaratan kata sandi untuk sistem file dan peran SVM

Anda dapat memperbarui persyaratan kata sandi untuk sistem file atau peran SVM menggunakan perintah `security login role config modify`ONTAPCLI. Perintah ini hanya tersedia untuk akun administrator sistem file dengan `fsxadmin` peran. Saat memodifikasi persyaratan kata sandi, sistem akan memperingatkan jika ada pengguna yang ada dengan peran itu yang akan terpengaruh oleh perubahan tersebut.

Contoh berikut memodifikasi persyaratan kata sandi panjang minimum menjadi 12 karakter untuk pengguna dengan `vsadmin-readonly` peran pada `fsx` SVM. Dalam contoh ini, ada pengguna yang sudah ada dengan peran ini.

```
FsxId0123456::> security login role config modify -role vsadmin-readonly -vserver fsx -
passwd-minlength 12
```

Sistem menampilkan peringatan berikut karena pengguna yang ada:

```
Warning: User accounts with this role exist. Modifications to the username/password
 restrictions on this role could result in non-compliant user
         accounts.
Do you want to continue? {y|n}:

FsxId0123456::>
```

Gagal memperbarui kata sandi **`fsxadmin`** akun

Saat memperbarui kata sandi untuk `fsxadmin` pengguna, Anda mungkin menerima kesalahan jika tidak memenuhi persyaratan kata sandi yang ditetapkan pada sistem file. Anda dapat melihat persyaratan kata sandi dengan menggunakan perintah `security login role config show` ONTAP CLI atau REST API.

Untuk melihat persyaratan kata sandi untuk sistem file atau peran SVM

1. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen Amazon fsX NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *`management_endpoint_ip`* dengan alamat IP port manajemen sistem file.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Untuk informasi selengkapnya, lihat Mengelola sistem file dengan ONTAP CLI.

2. `security login role config show`Perintah mengembalikan persyaratan kata sandi untuk sistem file atau peran SVM.

   ```
   FsxId0123456::> security login role config show -role fsxadmin -
   fields password_requirement_fields
   ```

Untuk `-fields` parameter, tentukan salah satu atau semua hal berikut:

- `passwd-minlength`— Panjang minimum kata sandi.
- `passwd-min-special-chars`— Jumlah minimum karakter khusus dalam kata sandi.
- `passwd-min-lowercase-chars`— Jumlah minimum karakter huruf kecil dalam kata sandi.
- `passwd-min-uppercase-chars`— Jumlah minimum karakter huruf besar dalam kata sandi.
- `passwd-min-digits`— Jumlah minimum digit dalam kata sandi.
- `passwd-alphanum`— Informasi tentang penyertaan atau pengecualian karakter alfanumerik.
- `passwd-expiry-time`— Waktu kedaluwarsa kata sandi.
- `passwd-expiry-warn-time`— Waktu peringatan kedaluwarsa kata sandi.

3. Jalankan perintah berikut untuk melihat semua persyaratan kata sandi:

```
FsxId0123456::> security login role config show -role fsxadmin -fields passwd-
minlength, passwd-min-special-chars, passwd-min-lowercase-chars, passwd-min-
digits, passwd-alphanum, passwd-expiry-time, passwd-expiry-warn-time, passwd-min-
uppercase-chars

vserver                role     passwd-minlength passwd-alphanum passwd-min-
special-chars passwd-expiry-time passwd-min-lowercase-chars passwd-min-uppercase-
chars passwd-min-digits passwd-expiry-warn-time
---------------------- -------- ---------------- ---------------
 ------------------------ ------------------ --------------------------
 -------------------------- ----------------- ----------------------
FsxId0123456           fsxadmin 3                enabled         0
       unlimited          0                        0                        0
               unlimited
```

Bermigrasi ke Amazon NetApp FSx untuk ONTAP

Bagian berikut memberikan informasi tentang cara memigrasi sistem file NetApp ONTAP yang ada ke Amazon FSx untuk ONTAP. NetApp

> **Note**
>
> Jika Anda berencana menggunakan kebijakan `All` tiering untuk memigrasikan data Anda ke tingkat kumpulan kapasitas, ingatlah bahwa metadata file selalu disimpan di tingkat SSD, dan semua data pengguna baru pertama kali ditulis ke tingkat SSD. Ketika data ditulis ke tingkat SSD, proses tiering latar belakang akan mulai meningkatkan data Anda ke penyimpanan kumpulan kapasitas, tetapi proses tiering tidak langsung dan menghabiskan sumber daya jaringan. Anda perlu mengukur tingkat SSD Anda untuk memperhitungkan metadata file (3-7% dari ukuran data pengguna), sebagai buffer untuk data pengguna sebelum berjenjang ke penyimpanan kolam kapasitas. Kami menyarankan agar Anda tidak melebihi 80% pemanfaatan tingkat SSD Anda.
> Saat memigrasikan data, pastikan untuk memantau tingkat SSD Anda menggunakan metrik sistem CloudWatch File untuk memastikan bahwa itu tidak mengisi lebih cepat daripada proses tiering dapat memindahkan data ke penyimpanan kumpulan kapasitas.

Topik

Migrasi ke FSx untuk ONTAP menggunakan NetApp SnapMirror

Anda dapat memigrasi sistem file NetApp ONTAP Anda ke Amazon FSx untuk ONTAP menggunakan. NetApp NetApp SnapMirror

NetApp SnapMirror menggunakan replikasi tingkat blok antara dua sistem file ONTAP, mereplikasi data dari volume sumber tertentu ke volume tujuan. Kami merekomendasikan penggunaan SnapMirror untuk memigrasikan sistem NetApp file ONTAP on-premise ke fsX untuk ONTAP. NetApp SnapMirrorreplikasi tingkat blok cepat dan efisien bahkan untuk sistem file dengan:

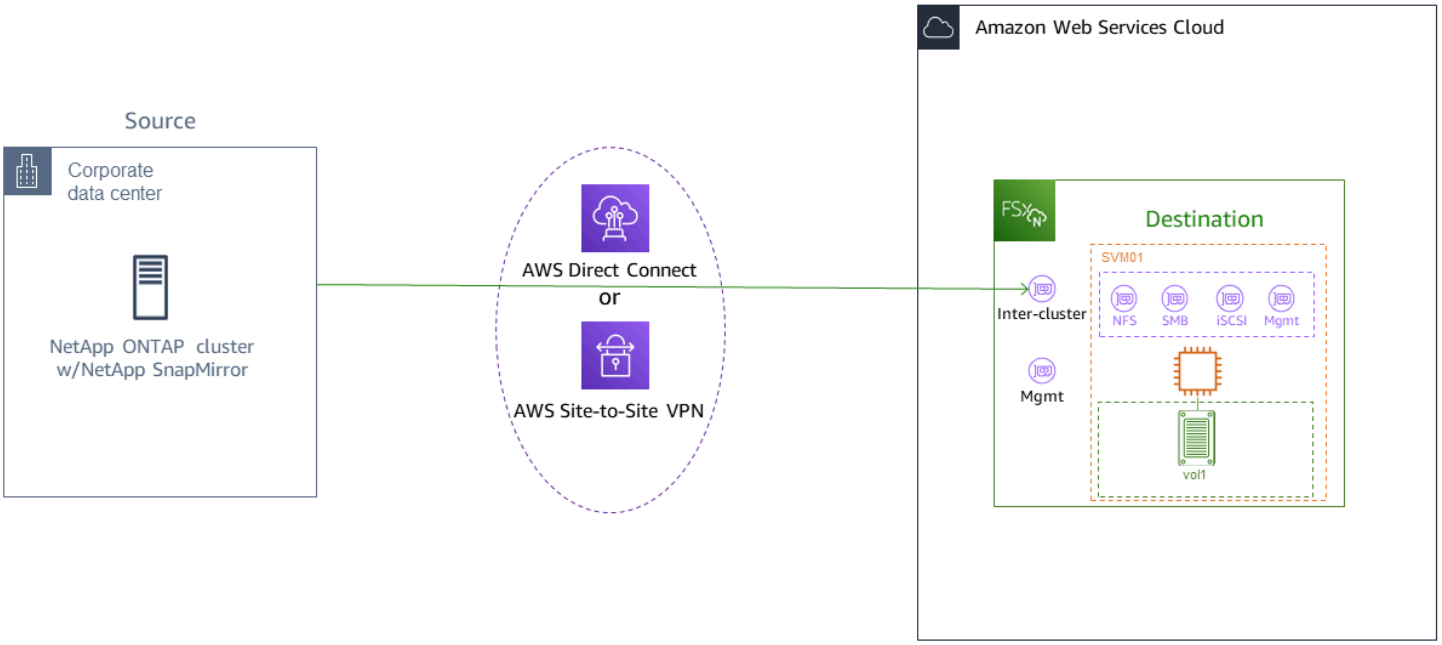
- Struktur direktori yang kompleks

- Lebih dari 50 juta file
- Ukuran file yang sangat kecil (sesuai urutan kilobyte)

Saat Anda menggunakan migrasi SnapMirror ke FSx untuk ONTAP, data yang tidak digandakan dan dikompresi tetap berada di status tersebut, yang mengurangi waktu transfer dan mengurangi jumlah bandwidth yang diperlukan untuk migrasi. Snapshot yang ada pada volume ONTAP sumber dipertahankan saat dimigrasikan ke volume tujuan. Memigrasi sistem file NetApp ONTAP lokal Anda ke FSx untuk ONTAP melibatkan tugas tingkat tinggi berikut:

1. Buat volume tujuan di Amazon FSx.
2. Kumpulkan antarmuka logis sumber dan tujuan (LIF).
3. Membangun cluster peering antara sumber dan sistem file tujuan.
4. Buat hubungan peering SVM.
5. Ciptakan SnapMirror hubungan.
6. Pertahankan klaster tujuan yang diperbarui.
7. Potong ke FSx Anda untuk sistem file ONTAP.

Diagram berikut menggambarkan skenario migrasi yang dijelaskan di bagian ini.



Topik

- Sebelum Anda memulai

- Buat volume tujuan
- Rekam LIF antar cluster sumber dan tujuan
- Membangun cluster peering antara sumber dan tujuan
- Buat hubungan peering SVM
- Ciptakan SnapMirror hubungan
- Transfer data ke FSx Anda untuk sistem file ONTAP
- Melakukan cut over ke Amazon FSx

Sebelum Anda memulai

Sebelum Anda mulai menggunakan prosedur yang dijelaskan di bagian berikut, pastikan Anda telah memenuhi prasyarat berikut:

- FSx untuk ONTAP memprioritaskan lalu lintas klien daripada tugas latar belakang termasuk tiering data, efisiensi penyimpanan, dan pencadangan. Saat memigrasikan data, dan sebagai praktik terbaik secara umum, kami menyarankan Anda memantau kapasitas tingkat SSD Anda untuk memastikan pemanfaatannya tidak melebihi 80%. Anda dapat memantau pemanfaatan tingkat SSD Anda menggunakan metrik sistem CloudWatch File. Untuk informasi selengkapnya, lihat Metrik volume.
- Jika Anda menyetel kebijakan tingkatan data volume tujuan `All` saat memigrasikan data, semua metadata file disimpan di tingkat penyimpanan SSD utama. Metadata file selalu disimpan di tingkat primer berbasis SSD, terlepas dari kebijakan tingkatan data volume. Kami menyarankan Anda mengasumsikan rasio 1:10 untuk tingkat primer: kapasitas kapasitas kapasitas kapasitas kapasitas penyimpanan tingkat.
- Sistem file sumber dan tujuan terhubung dalam VPC yang sama, atau berada di jaringan yang diintip menggunakan Amazon VPC Peering, Transit Gateway, atau. AWS Direct Connect AWS VPN Untuk informasi lebih lanjut, lihat Mengakses data dari dalam AWS dan Apa itu VPC peering? di Panduan Peering VPC Amazon.
- Grup keamanan VPC untuk sistem file FSx untuk ONTAP memiliki aturan masuk dan keluar yang memungkinkan ICMP serta TCP pada port 443, 10000, 11104, dan 11105 untuk titik akhir antar-cluster (LIF) Anda.
- Verifikasi bahwa volume sumber dan tujuan menjalankan versi NetApp ONTAP yang kompatibel sebelum membuat hubungan perlindungan SnapMirror data. Untuk informasi selengkapnya, lihat Versi ONTAP yang kompatibel untuk SnapMirror hubungan dalam dokumentasi NetApp pengguna

ONTAP. Prosedur yang disajikan di sini menggunakan sistem file NetApp ONTAP on-premise untuk sumbernya.

- Sistem file NetApp ONTAP lokal (sumber) Anda menyertakan lisensi. SnapMirror
- Anda telah membuat FSx tujuan untuk sistem file ONTAP dengan SVM, tetapi Anda belum membuat volume tujuan. Untuk informasi selengkapnya, lihat Membuat fsX untuk sistem file ONTAP.

Perintah dalam prosedur ini menggunakan alias klaster, SVM, dan volume berikut:

- *FSx-Dest*— ID cluster tujuan (FSx) (dalam format F SxIdabcdef 1234567890a).
- *OnPrem-Source*— ID cluster sumber.
- *DestSVM*— nama SVM tujuan.
- *SourceSVM*— nama sumber SVM.
- Baik nama volume sumber dan tujuan adalah`vol1`.

> **Note**
>
> Sebuah fsX untuk sistem file ONTAP disebut sebagai cluster di semua perintah ONTAP CLI.

Prosedur di bagian ini menggunakan perintah CLI NetApp ONTAP berikut.

- volume membuat perintah
- perintah cluster
- perintah rekan vserver
- perintah snapmirror

Anda akan menggunakan CLI NetApp ONTAP untuk membuat dan mengelola SnapMirror konfigurasi pada fsX Anda untuk sistem file ONTAP. Untuk informasi selengkapnya, lihat Menggunakan CLI NetApp ONTAP.

Buat volume tujuan

Anda dapat membuat volume tujuan perlindungan data (DP) menggunakan konsol Amazon FSx, API, AWS CLI dan Amazon fsX, selain NetApp ONTAP CLI dan REST API. Untuk informasi tentang membuat volume tujuan menggunakan konsol Amazon FSx danAWS CLI, lihat. Membuat volume

Dalam prosedur berikut, Anda akan menggunakan CLI NetApp ONTAP untuk membuat volume tujuan pada fsX Anda untuk sistem file ONTAP. Anda akan memerlukan `fsxadmin` kata sandi dan alamat IP atau nama DNS dari port manajemen sistem file.

1. Buat sesi SSH dengan sistem file tujuan menggunakan pengguna `fsxadmin` dan kata sandi yang Anda tetapkan saat Anda membuat sistem file.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Buat volume pada cluster tujuan yang memiliki kapasitas penyimpanan yang setidaknya sama dengan kapasitas penyimpanan volume sumber. Gunakan `-type DP` untuk menunjuknya sebagai tujuan untuk suatu SnapMirror hubungan.

   Jika Anda berencana untuk menggunakan tiering data, kami sarankan Anda `-tiering-policy` menyetelnya. `all` Ini memastikan bahwa data Anda segera ditransfer ke penyimpanan kolam kapasitas dan mencegah Anda kehabisan kapasitas pada tingkat SSD Anda. Setelah migrasi, Anda dapat beralih `-tiering-policy` ke`auto`.

   > **Note**
   >
   > Metadata file selalu disimpan di tingkat primer berbasis SSD, terlepas dari kebijakan tingkatan data volume.

   ```
   FSx-Dest::> vol create -vserver DestSVM -volume vol1 -aggregate aggr1 -size 1g -
   type DP -tiering-policy all
   ```

Rekam LIF antar cluster sumber dan tujuan

SnapMirror menggunakan antarmuka logis antar-cluster (LIF), masing-masing dengan alamat IP unik, untuk memfasilitasi transfer data antara cluster sumber dan tujuan.

1. Untuk FSx tujuan untuk sistem file ONTAP, Anda dapat mengambil titik akhir Inter-cluster - alamat IP dari konsol Amazon FSx dengan menavigasi ke tab Administrasi di halaman detail sistem file Anda.
2. Untuk cluster NetApp ONTAP sumber, ambil alamat IP LIF antar-cluster menggunakan CLI ONTAP. Jalankan perintah berikut:

```
OnPrem-Source::> network interface show -role intercluster

Logical                         Network
Vserver     Interface  Status  Address/Mask
----------- ---------- ------- ------------
FSx-Dest
             inter_1    up/up  10.0.0.36/24
             inter_2    up/up  10.0.1.69/24
```

> **Note**
>
> Untuk sistem file scale-out, ada dua alamat IP antar-cluster untuk setiap pasangan ketersediaan tinggi (HA). Simpan nilai-nilai ini untuk nanti.

Simpan alamat `inter_1` dan `inter_2` IP. Mereka direferensikan dalam `FSx-Dest` as `dest_inter_1` dan `dest_inter_2` dan untuk `OnPrem-Source` as `source_inter_1` dan`source_inter_2`.

Membangun cluster peering antara sumber dan tujuan

Menetapkan hubungan peer cluster pada cluster tujuan dengan menyediakan alamat IP antar-cluster. Anda juga perlu membuat frasa sandi yang harus Anda masukkan saat Anda membuat cluster peering di cluster sumber.

1. Siapkan peering pada cluster tujuan menggunakan perintah berikut. Untuk sistem file scale-out, Anda harus memberikan setiap alamat IP antar-cluster.

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-
addrs source_inter_1,source_inter_2

Enter the passphrase:
```

```
Confirm the passphrase:
Notice: Now use the same passphrase in the "cluster peer create" command in the
 other cluster.
```

2. Selanjutnya, buat hubungan rekan cluster pada cluster sumber. Anda harus memasukkan frasa sandi yang Anda buat di atas untuk mengautentikasi. Untuk sistem file scale-out, Anda harus memberikan setiap alamat IP antar-cluster.

```
OnPrem-Source::> cluster peer create -address-family ipv4 -peer-
addrs dest_inter_1,dest_inter_2

Enter the passphrase:
Confirm the passphrase:
```

3. Verifikasi peering berhasil menggunakan perintah berikut pada cluster sumber. Dalam output, `Availability` harus diatur ke`Available`.

```
OnPrem-Source::> cluster peer show

Peer Cluster Name  Availability   Authentication
-----------------  -------------- --------------
FSx-Dest           Available      ok
```

Buat hubungan peering SVM

Dengan pengintip cluster didirikan, langkah selanjutnya adalah mengintip SVM. Buat hubungan peering SVM pada cluster tujuan (FSX-dest) menggunakan perintah. `vserver peer` Alias tambahan yang digunakan dalam perintah berikut adalah sebagai berikut:

- `DestLocalName`— ini adalah nama yang digunakan untuk mengidentifikasi SVM tujuan saat mengkonfigurasi SVM mengintip pada sumber SVM.
- `SourceLocalName`— ini adalah nama yang digunakan untuk mengidentifikasi sumber SVM saat mengkonfigurasi SVM mengintip pada SVM tujuan.

1. Gunakan perintah berikut untuk membuat hubungan peering SVM antara SVM sumber dan tujuan.

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver SourceSVM -peer-
cluster OnPrem-Source -applications snapmirror -local-name SourceLocalName
```

```
 Info: [Job 207] 'vserver peer create' job queued
```

2. Terima hubungan peering di cluster sumber:

```
OnPrem-Source::> vserver peer accept -vserver SourceSVM -peer-vserver DestSVM -
local-name DestLocalName

 Info: [Job 211] 'vserver peer accept' job queued
```

3. Verifikasi status peering SVM menggunakan perintah berikut; `Peer State` harus diatur ke `peered` dalam respons.

```
OnPrem-Source::> vserver peer show

Peer    Peer     Peer   Peering  Remote
vserver Vserver  State  Cluster  Applications  Vserver
------- -------- ------ -------- ------------ ---------
svm01   destsvm1 peered FSx-Dest snapmirror    svm01
```

Ciptakan SnapMirror hubungan

Sekarang setelah Anda mengintip SVM sumber dan tujuan, langkah selanjutnya adalah membuat dan menginisialisasi SnapMirror hubungan pada cluster tujuan.

> **Note**
>
> Setelah Anda membuat dan menginisialisasi SnapMirror hubungan, volume tujuan hanya dapat dibaca sampai hubungan terputus.

- Gunakan `snapmirror create` perintah untuk membuat SnapMirror hubungan pada cluster tujuan. `snapmirror create`Perintah harus digunakan dari SVM tujuan.

  Anda dapat secara opsional menggunakan `-throttle` untuk mengatur bandwidth maksimum (dalam KB/detik) untuk hubungan. SnapMirror

```
FSx-Dest::> snapmirror create -source-path SourceLocalName:vol1 -destination-
path DestSVM:vol1 -vserver DestSVM -throttle unlimited
```

```
Operation succeeded: snapmirror create for the relationship with destination
"DestSVM:vol1".
```

Transfer data ke FSx Anda untuk sistem file ONTAP

Sekarang setelah Anda membuat SnapMirror hubungan, Anda dapat mentransfer data ke sistem file tujuan.

1. Anda dapat mentransfer data ke sistem file tujuan dengan menjalankan perintah berikut pada sistem file tujuan.

   > **Note**
   >
   > Setelah Anda menjalankan perintah ini, SnapMirror mulai mentransfer snapshot data dari volume sumber ke volume tujuan.

   ```
   FSx-Dest::> snapmirror initialize -destination-path DestSVM:vol1 -source-
   path SourceLocalName:vol1
   ```

2. Jika Anda memigrasikan data yang sedang digunakan secara aktif, Anda harus memperbarui klaster tujuan agar tetap disinkronkan dengan cluster sumber Anda. Untuk melakukan pembaruan satu kali ke cluster tujuan, jalankan perintah berikut.

   ```
   FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
   ```

3. Anda juga dapat menjadwalkan pembaruan setiap jam atau harian sebelum menyelesaikan migrasi dan memindahkan klien Anda ke FSx untuk ONTAP. Anda dapat membuat jadwal SnapMirror pembaruan menggunakan `snapmirror modify`perintah.

   ```
   FSx-Dest::> snapmirror modify -destination-path DestSVM:vol1 -schedule hourly
   ```

Melakukan cut over ke Amazon FSx

Untuk mempersiapkan pemotongan ke FSx Anda untuk sistem file ONTAP, lakukan hal berikut:

- Putuskan sambungan semua klien yang menulis ke cluster sumber.

- Lakukan SnapMirror transfer akhir untuk memastikan tidak ada kehilangan data saat memotong.
- Putuskan SnapMirror hubungan.
- Hubungkan semua klien ke FSx Anda untuk sistem file ONTAP.

1. Untuk memastikan bahwa semua data dari cluster sumber ditransfer ke FSx untuk sistem file ONTAP, lakukan transfer Snapmirror akhir.

```
FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
```

2. Pastikan migrasi data selesai dengan memverifikasi yang `Mirror State` disetel ke`Snapmirrored`, dan `Relationship Status` disetel ke`Idle`. Anda juga harus memastikan bahwa `Last Transfer End Timestamp` tanggalnya seperti yang diharapkan, seperti yang ditunjukkan kapan transfer terakhir ke volume tujuan terjadi.
3. Jalankan perintah berikut untuk menunjukkan SnapMirror status.

```
FSx-Dest::> snapmirror show -fields state,status,last-transfer-end-timestamp

Source     Destination   Mirror        Relationship Last Transfer End
Path       Path          State         Status       Timestamp
---------- -----------   ----------    -------      ---------------
Svm01:vol1 svm02:DestVol Snapmirrored  Idle         09/02 09:02:21
```

4. Nonaktifkan SnapMirror transfer future apa pun dengan menggunakan `snapmirror quiesce` perintah.

```
FSx-Dest::> snapmirror quiesce -destination-path DestSVM:vol1
```

5. Verifikasi bahwa `Relationship Status` telah berubah menjadi `Quiesced` penggunaan`snapmirror show`.

```
FSx-Dest::> snapmirror show

Source           Destination   Mirror        Relationship
Path             Path          State         Status
-----------      ------------  ------------- --------
sourcesvm1:vol1  svm01:DestVol Snapmirrored  Quiesced
```

6. Selama migrasi, volume tujuan hanya-baca. Untuk mengaktifkan baca/tulis, Anda perlu memutuskan SnapMirror hubungan dan memotong ke FSx Anda untuk sistem file ONTAP. Putuskan SnapMirror hubungan menggunakan perintah berikut.

```
FSx-Dest::> snapmirror break -destination-path DestSVM:vol1

Operation succeeded: snapmirror break for destination "DestSVM:vol1".
```

7. Setelah SnapMirror replikasi selesai dan Anda telah memutuskan SnapMirror hubungan, Anda dapat memasang volume untuk membuat data tersedia.

```
FSx-Dest::> vol mount -vserver fsx -volume vol1 -junction-path /vol1
```

Volume sekarang tersedia dengan data dari volume sumber yang sepenuhnya dimigrasikan ke volume tujuan Volume juga tersedia bagi klien untuk membaca dan menulis ke sana. Jika sebelumnya Anda mengatur `tiering-policy` volume ini`all`, Anda dapat mengubahnya menjadi `auto` atau `snapshot-only` dan data Anda akan secara otomatis bertransisi antar tingkatan penyimpanan sesuai dengan pola akses. Untuk membuat data ini dapat diakses oleh klien dan aplikasi, lihatMengakses data.

Migrasi ke FSx untuk ONTAP menggunakan AWS DataSync

Sebaiknya gunakan AWS DataSync untuk mentransfer data antara FSx untuk sistem file ONTAP dan sistem file non-ONTAP, termasuk FSx for Lustre, FSx untuk OpenZFS, FSx for Windows File Server, Amazon EFS, Amazon S3, dan filer lokal. Jika Anda mentransfer file antara FSx untuk ONTAP NetApp dan ONTAP, sebaiknya gunakan. NetApp SnapMirror AWS DataSyncadalah layanan transfer data yang menyederhanakan, mengotomatisasi, dan mempercepat pemindahan dan replikasi data antara sistem penyimpanan yang dikelola sendiri dan layanan AWS penyimpanan melalui internet atau. AWS Direct Connect DataSync dapat mentransfer data dan metadata sistem file Anda, seperti kepemilikan, stempel waktu, dan izin akses.

Anda dapat menggunakan DataSync untuk mentransfer file antara dua FSx untuk sistem file ONTAP, dan juga memindahkan data ke sistem file di akun yang berbeda Wilayah AWS atau. AWS Anda juga dapat menggunakan DataSync dengan FSx untuk sistem file ONTAP untuk tugas-tugas lain. Misalnya, Anda dapat melakukan migrasi data satu kali, secara berkala menyerap data untuk beban kerja yang terdistribusi, dan menjadwalkan replikasi untuk perlindungan dan pemulihan data.

Di DataSync, lokasi adalah titik akhir untuk FSx untuk sistem file ONTAP. Untuk informasi tentang skenario transfer tertentu, lihat Bekerja dengan lokasi di Panduan AWS DataSync Pengguna.

> **Note**
>
> Jika Anda berencana menggunakan kebijakan `All` tiering untuk memigrasikan data Anda ke tingkat kumpulan kapasitas, ingatlah bahwa metadata file selalu disimpan di tingkat SSD, dan semua data pengguna baru pertama kali ditulis ke tingkat SSD. Ketika data ditulis ke tingkat SSD, proses tiering latar belakang akan mulai meningkatkan data Anda ke penyimpanan kumpulan kapasitas, tetapi proses tiering tidak langsung dan menghabiskan sumber daya jaringan. Anda perlu mengukur tingkat SSD Anda untuk memperhitungkan metadata file (3-7% dari ukuran data pengguna), sebagai buffer untuk data pengguna sebelum berjenjang ke penyimpanan kolam kapasitas. Kami menyarankan Anda untuk tidak melebihi 80% pemanfaatan SSD.
> Saat memigrasikan data, pastikan untuk memantau tingkat SSD Anda menggunakan metrik sistem CloudWatch File untuk memastikan bahwa itu tidak mengisi lebih cepat daripada proses tiering dapat memindahkan data ke penyimpanan kumpulan kapasitas. Anda juga dapat membatasi DataSync transfer ke tingkat yang lebih rendah dari tingkat tiering yang terjadi untuk memastikan bahwa tingkat SSD Anda tidak melebihi penggunaan 80%. Misalnya, untuk sistem file dengan kapasitas throughput minimal 512 MBps, throttle 200 MBps biasanya akan menyeimbangkan transfer data dan kecepatan tiering data.

Prasyarat

Untuk memigrasikan data ke FSx Anda untuk penyiapan ONTAP, Anda memerlukan server dan jaringan yang memenuhi persyaratan. DataSync Untuk mempelajari lebih lanjut, lihat Persyaratan untuk DataSync di Panduan AWS DataSync Pengguna.

Langkah-langkah dasar untuk memigrasi file menggunakan DataSync

Mentransfer file dari sumber ke tujuan menggunakan DataSync melibatkan langkah-langkah dasar berikut:

- Unduh dan gunakan agen di lingkungan Anda dan aktifkan (tidak diperlukan jika mentransfer antarLayanan AWS).
- Buat lokasi sumber dan tujuan.
- Buat tugas.

- Jalankan tugas untuk mentransfer file dari sumber ke tujuan.

Untuk informasi selengkapnya, lihat topik berikut di Panduan Pengguna AWS DataSync:

- Transfer data antara penyimpanan yang dikelola sendiri dan AWS
- Membuat lokasi untuk Amazon FSx untuk ONTAP NetApp

Memantau Amazon FSx untuk ONTAP NetApp

Anda dapat menggunakan layanan dan alat berikut untuk memantau Amazon FSx untuk penggunaan dan aktivitas NetApp ONTAP:

- Amazon CloudWatch — Anda dapat memantau sistem file menggunakan Amazon CloudWatch, yang secara otomatis mengumpulkan dan memproses data mentah dari FSx untuk ONTAP menjadi metrik yang dapat dibaca. Statistik ini disimpan untuk jangka waktu 15 bulan sehingga Anda dapat mengakses informasi historis dan melihat kinerja sistem file Anda. Anda juga dapat menyetel alarm berdasarkan metrik selama periode waktu tertentu dan melakukan satu atau beberapa tindakan berdasarkan nilai metrik relatif terhadap ambang batas yang Anda tentukan.
- Acara ONTAP EMS - Anda dapat memantau FSx Anda untuk sistem file ONTAP dengan menggunakan peristiwa yang dihasilkan oleh Sistem Manajemen Acara (EMS) ONTAP. Peristiwa EMS adalah pemberitahuan kejadian di sistem file Anda, seperti pembuatan iSCSI LUN atau ukuran volume otomatis.
- NetApp Cloud Insights — Anda dapat memantau metrik konfigurasi, kapasitas, dan kinerja untuk fsX untuk sistem file ONTAP menggunakan layanan Cloud Insights. NetApp Anda juga dapat membuat peringatan berdasarkan kondisi metrik.
- NetApp Harvest dan NetApp Grafana — Anda dapat memantau FSx Anda untuk sistem file ONTAP dengan menggunakan Harvest dan Grafana. NetApp NetApp NetApp Harvest memantau sistem file ONTAP dengan mengumpulkan metrik kinerja, kapasitas, dan perangkat keras dari FSx untuk sistem file ONTAP. Grafana menyediakan dasbor tempat metrik Harvest yang dikumpulkan dapat ditampilkan.
- AWS CloudTrail— Anda dapat menggunakan AWS CloudTrail untuk menangkap semua panggilan API untuk Amazon FSx sebagai acara. Peristiwa ini memberikan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Amazon FSx.

Topik

Pemantauan CloudWatch dengan Amazon

Anda dapat memantau sistem file menggunakan Amazon CloudWatch, yang mengumpulkan dan memproses data mentah dari Amazon FSx NetApp untuk ONTAP menjadi metrik hampir real-time yang dapat dibaca. Statistik ini disimpan untuk jangka waktu 15 bulan, sehingga Anda dapat mengakses informasi historis untuk menentukan kinerja sistem file Anda. FSx untuk data metrik ONTAP secara otomatis dikirim ke periode 1 menit CloudWatch secara default. Untuk informasi selengkapnya CloudWatch, lihat Apa itu Amazon CloudWatch? di Panduan CloudWatch Pengguna Amazon.

> **Note**
>
> Secara default, FSx untuk ONTAP mengirimkan data CloudWatch metrik ke periode 1 menit kecuali untuk metrik berikut yang dikirim dalam interval 5 menit:
>
> - `FileServerDiskThroughputBalance`
> - `FileServerDiskIopsBalance`

CloudWatch metrik untuk FSx untuk ONTAP disusun menjadi empat kategori, yang ditentukan oleh dimensi yang digunakan untuk menanyakan setiap metrik. Untuk informasi selengkapnya tentang dimensi, lihat Dimensi di Panduan CloudWatch Pengguna Amazon.

- Metrik sistem file: Metrik ile-system-level kinerja dan kapasitas penyimpanan F.
- Metrik sistem file terperinci: Metrik ile-system-level penyimpanan F per tingkat penyimpanan (SSD dan kumpulan kapasitas).
- Metrik volume: Kinerja per volume dan metrik kapasitas penyimpanan.
- Metrik volume terperinci: Metrik kapasitas penyimpanan per volume berdasarkan tingkat penyimpanan atau menurut jenis data (pengguna, snapshot, atau lainnya).

Semua CloudWatch metrik untuk FSx untuk ONTAP dipublikasikan ke `AWS/FSx` namespace di. CloudWatch

Topik

- Cara menggunakan fsX untuk metrik ONTAP CloudWatch
- Mengakses metrik CloudWatch

- Metrik sistem file
- Metrik sistem file scale-out
- Metrik volume
- Peringatan dan rekomendasi kinerja
- Membuat CloudWatch alarm Amazon untuk memantau Amazon FSx

Cara menggunakan fsX untuk metrik ONTAP CloudWatch

CloudWatch Metrik yang dilaporkan oleh Amazon FSx memberikan informasi berharga tentang fsX Anda untuk sistem dan volume file ONTAP.

Topik

- Memantau metrik sistem file di konsol Amazon FSx
- Memantau metrik volume di konsol Amazon FSx

Memantau metrik sistem file di konsol Amazon FSx

Anda dapat menggunakan panel Pemantauan & kinerja di dasbor sistem file Anda di konsol Amazon FSx untuk melihat metrik yang dijelaskan dalam tabel berikut. Untuk informasi selengkapnya, lihat Mengakses metrik CloudWatch .

Pemantau & kinerja	Bagaimana saya...	Bagan	Metrik terkait
Ringkasan	... menentukan jumlah kapasitas penyimpanan yang tersedia pada sistem file saya?	Kapasitas penyimpanan primer yang tersedia (byte)	`StorageCapacity {SSD} - StorageUsed {SSD}`
	... menentukan total throughput klien sistem file saya?	Total throughput klien	SUM (`DataReadBytes +DataWriteBytes`) /PERIODE (dalam detik)

Pemanta n & kinerja	Bagaimana saya...	Bagan	Metrik terkait
		(byte/detik)	
	... menentukan IOPS klien total sistem file saya?	Total IOPS klien (operasi/detik)	SUM (`DataRead0perations + DataWriteOperations +MetadataOperations`) /PERIODE (dalam detik)
	... menentukan latensi rata-rata untuk operasi baca, tulis, dan metadata sistem file saya?	Latensi rata-rata (ms/operasi)	Latensi baca rata-rata: `DataReadOperationTime` * 1000/ `DataRead0perations` Latensi tulis rata-rata: `DataWriteOperationTime` * 1000/ `DataWriteOperations` Latensi metadata rata-rata: * 1000/ `Metadata0perationTime MetadataOperations`

Pemantauan & kinerja	Bagaimana saya...	Bagan	Metrik terkait
Penyimpanan	... menentukan distribusi kapasitas penyimpanan bekas dan gratis pada sistem file saya?	Distribusi penyimpanan	Tingkat utama tersedia: `StorageCapacity {SSD} - StorageUsed {SSD}` Tingkat primer yang digunakan: `StorageUsed {SSD}` Kolam kapasitas yang digunakan: `StorageUsed {StandardCapacityPool }`
	... menentukan penghematan dari efisiensi penyimpanan (kompresi, deduplikasi, dan pemadatan)?	Penghematan efisiensi penyimpanan	`StorageEfficiencySavings`
	... menentukan berapa banyak penyimpanan primer yang tersedia?	Kapasitas penyimpanan primer yang tersedia (byte)	`StorageCapacity {SSD} - StorageUsed {SSD}`
	... menentukan persen penyimpanan primer yang digunakan untuk sistem file saya?	Pemanfaatan kapasitas penyimpanan primer (persen)	`StorageUsed {SSD} * 100/ StorageCapacity {} SSD`

Pemanta n & kinerja	Bagaimana saya...	Bagan	Metrik terkait
	... menentukan apakah sistem file saya mendekati batas throughput jaringannya?	Throughput jaringan - pemanfaatan (persen)	`NetworkThroughputUtilization`
	... tentukan apakah sistem file saya mendekati batas throughput disknya?	Disk throughput — pemanfaatan (persen)	`FileServerDiskThroughputUtilization`
Kinerja server file	... tentukan apakah sistem file saya telah kehabisan kredit burst yang diizinkan untuk throughput disk?	Throughput disk — keseimbangan burst (persen)	`FileServerDiskThroughputBalance`
	... tentukan apakah sistem file saya mendekati batas IOPS SSD server file-nya?	Disk IOPS - pemanfaatan (persen)	`FileServerDiskIopsUtilization`
	... tentukan apakah sistem file saya telah kehabisan kredit burst yang diizinkan server file-nya untuk disk SSD IOPS?	Disk IOPS — keseimbangan burst (persen)	`FileServerDiskIopsBalance`

Pemanta n & kinerja	Bagaimana saya...	Bagan	Metrik terkait
	... menentukan rata-rata pemanfaatan CPU sistem file?	Pemanfaat an CPU (persen)	`CPUUtilization`
	... menentukan apakah beban kerja saya memanfaatkan RAM sistem file saya dan cache baca NVMe secara efisien?	Rasio hit cache (persen)	`FileServerCacheHit Ratio`
Perform disk	... tentukan apakah sistem file saya mendekati kapasitas IOPS SSD yang saat ini disediakan?	Disk IOPS - pemanfaat an (SSD) (persen)	`DiskIopsUtilization`

> **Note**
>
> Kami menyarankan Anda mempertahankan pemanfaatan kapasitas throughput rata-rata dari setiap dimensi terkait kinerja seperti pemanfaatan jaringan, pemanfaatan CPU, dan pemanfaatan SSD IOPS hingga di bawah 50%. Ini memastikan bahwa Anda memiliki kapasitas throughput cadangan yang cukup untuk lonjakan tak terduga dalam beban kerja Anda, serta untuk setiap operasi penyimpanan latar belakang (seperti sinkronisasi penyimpanan, tiering data, atau cadangan).

Memantau metrik volume di konsol Amazon FSx

Anda dapat melihat panel Pemantauan di dasbor volume Anda di konsol Amazon FSx untuk melihat metrik kinerja tambahan. Untuk informasi selengkapnya, lihat Mengakses metrik CloudWatch .

Pemanta n	Bagaimana saya...	Bagan	Metrik terkait
	... menentukan kapasitas penyimpanan volume saya yang tersedia?	Kapasitas penyimpan an yang tersedia	`StorageCapacity`
	... menentukan total throughput klien volume saya?	Total throughpu t klien (byte/det ik)	SUM (`DataReadB ytes +DataWrite Bytes`) /PERIODE (dalam detik)
	... menentukan total IOPS klien volume saya?	Total IOPS klien (operasi/ detik)	SUM (`DataRead0 perations + DataWriteOperations +MetadataOperations`) /PERIODE (dalam detik)
	... menentukan berapa banyak operasi baca dan tulis yang berasal dari atau pergi ke tingkat kumpulan kapasitas?	Kapasitas Kolam IOPS (operasi/ detik)	Baca operasi: `CapacityP oolRead0perations` Tulis operasi: `CapacityP oolWriteOperations`
	... menentukan latensi rata-rata untuk operasi baca, tulis, dan metadata volume saya?	Latensi rata- rata (ms/ operasi)	Latensi baca rata-rata: `DataRead0perationT ime` * 1000/ `DataRead0 perations` Latensi tulis rata-rata: `DataWriteOperation Time` * 1000/ `DataWrite 0perations` Latensi metadata rata- rata: * 1000/ `Metadata0`

Pemanta n	Bagaimana saya...	Bagan	Metrik terkait
			`perationTime MetadataOperations`
	... menentukan jumlah file atau inode yang tersedia pada volume saya?	File yang tersedia (inode)	`FilesCapacity - FilesUsed`
	... menentukan distribusi kapasitas penyimpanan bekas dan gratis pada volume saya?	Distribusi penyimpan an	`StorageCapacity - StorageUsed`

Mengakses metrik CloudWatch

Anda dapat melihat CloudWatch metrik Amazon untuk Amazon FSx dengan cara berikut:

- Konsol Amazon FSx
- CloudWatch Konsol Amazon
- AWS Command Line Interface (AWS CLI) untuk CloudWatch
- CloudWatch API

Prosedur berikut menjelaskan cara melihat CloudWatch metrik sistem file Anda dengan konsol Amazon FSx.

Untuk melihat CloudWatch metrik untuk sistem file Anda menggunakan konsol Amazon FSx

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Di panel navigasi kiri, pilih Sistem file, lalu pilih sistem file yang metriknya ingin Anda lihat.
3. Pada halaman Ringkasan, pilih Pemantauan & kinerja dari panel kedua untuk melihat grafik untuk metrik sistem file Anda.

Ada empat tab pada panel Monitoring & Performance.

- Pilih Ringkasan (tab default) untuk menampilkan peringatan aktif, CloudWatch alarm, dan grafik untuk aktivitas sistem File.
- Pilih Penyimpanan untuk melihat kapasitas penyimpanan dan metrik pemanfaatan.
- Pilih Kinerja untuk melihat metrik kinerja server file dan penyimpanan.
- Pilih CloudWatch alarm untuk melihat grafik alarm apa pun yang dikonfigurasi untuk sistem file Anda.

Prosedur berikut menjelaskan cara melihat CloudWatch metrik volume Anda dengan konsol Amazon FSx

Untuk melihat CloudWatch metrik volume Anda menggunakan konsol Amazon FSx

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Di panel navigasi kiri, pilih Volume, lalu pilih volume yang metriknya ingin Anda lihat.
3. Pada halaman Ringkasan, pilih Monitoring (tab default) dari panel kedua untuk melihat grafik untuk metrik volume Anda.

Prosedur berikut menjelaskan cara melihat CloudWatch metrik sistem file Anda dengan CloudWatch konsol Amazon.

Untuk melihat metrik menggunakan konsol Amazon CloudWatch

1. Pada halaman Ringkasan sistem file Anda, pilih Pemantauan & kinerja dari panel kedua untuk melihat grafik untuk metrik sistem file Anda.
2. Pilih Lihat dalam metrik dari menu tindakan di kanan atas grafik yang ingin Anda lihat di CloudWatch konsol Amazon. Ini membuka halaman Metrik di CloudWatch konsol Amazon.

Prosedur berikut menjelaskan cara menambahkan fsX untuk metrik sistem file ONTAP ke dasbor di konsol Amazon. CloudWatch

Untuk menambahkan metrik ke konsol Amazon CloudWatch

1. Pilih kumpulan metrik (Ringkasan, Penyimpanan, atau Kinerja) di panel Pemantauan & kinerja konsol Amazon FSx.
2. Pilih Tambahkan ke dasbor di kanan atas panel. Ini membuka CloudWatch konsol Amazon.

3. Pilih CloudWatch dasbor yang ada dari daftar, atau buat dasbor baru. Untuk informasi selengkapnya, lihat Menggunakan CloudWatch dasbor Amazon di Panduan CloudWatch Pengguna Amazon.

Prosedur berikut menjelaskan cara mengakses metrik sistem file Anda dengan. AWS CLI

Untuk mengakses metrik dari AWS CLI

- Gunakan perintah CLI CloudWatch daftar-metrik dengan parameter. `--namespace "AWS/FSx"` Untuk informasi selengkapnya, lihat Referensi Perintah AWS AWS CLI.

Prosedur berikut menjelaskan cara mengakses metrik sistem file Anda dengan CloudWatch API.

Untuk mengakses metrik dari API CloudWatch

- Panggil operasi API GetMetricStatistik. Untuk informasi selengkapnya, lihat Referensi Amazon CloudWatch API.

Metrik sistem file

Metrik sistem file Amazon FSx untuk NetApp ONTAP Anda diklasifikasikan sebagai metrik sistem file atau metrik sistem file terperinci.

- Metrik sistem file adalah metrik kinerja dan penyimpanan agregat untuk satu sistem file yang mengambil satu dimensi. `FileSystemId` Metrik ini mengukur kinerja jaringan dan penggunaan kapasitas penyimpanan untuk sistem file Anda.
- Metrik sistem file terperinci mengukur kapasitas penyimpanan sistem file Anda dan penyimpanan yang digunakan di setiap tingkat penyimpanan (misalnya, penyimpanan SSD dan penyimpanan kolam kapasitas). Setiap metrik mencakup`FileSystemId`,`StorageTier`, dan `DataType` dimensi.

Perhatikan hal berikut tentang kapan Amazon FSx menerbitkan titik data untuk metrik ini ke: CloudWatch

- Untuk metrik pemanfaatan (metrik apa pun yang namanya diakhiri dengan Pemanfaatan, seperti`NetworkThroughputUtilization`), ada titik data yang dipancarkan setiap periode untuk setiap server file aktif atau agregat. Misalnya, Amazon FSx memancarkan satu metrik kecil per

server file aktif untuk`FileServerDiskIopsUtilization`, dan satu metrik kecil per agregat untuk. `DiskIopsUtilization`

- Untuk semua metrik lainnya, ada satu titik data yang dipancarkan setiap periode, sesuai dengan nilai total metrik di semua server file aktif Anda (seperti `DataReadBytes` untuk metrik server file) atau semua agregat Anda (seperti `DiskReadBytes` untuk metrik penyimpanan).

Topik

Metrik I/O jaringan

Semua metrik ini mengambil satu dimensi,`FileSystemId`.

Metrik	Deskripsi
`NetworkThroughputUtilization`	Persentase pemanfaatan throughput jaringan untuk sistem file. `Average`Statistik adalah pemanfaatan throughput jaringan rata-rata dari sistem file selama periode tertentu. `Minimum`Statistik adalah pemanfaatan throughput jaringan terendah dari sistem file selama periode tertentu. `Maximum`Statistik adalah pemanfaatan throughput jaringan tertinggi dari sistem file selama periode tertentu. Unit: Persen

Metrik	Deskripsi
	Statistik yang valid:`Average`,`Minimum`, dan `Maximum`
`NetworkSentBytes`	Jumlah byte (jaringan I/O) yang dikirim oleh sistem file. `Sum`Statistik adalah jumlah total byte yang dikirim oleh sistem file selama periode tertentu. Untuk menghitung throughput terkirim (byte per detik) untuk statistik apa pun, bagilah statistik dengan detik dalam periode yang ditentukan. Unit: Bita Statistik valid: `Sum`
`NetworkReceivedBytes`	Jumlah byte (jaringan I/O) yang diterima oleh sistem file. `Sum`Statistik adalah jumlah total byte yang diterima oleh sistem file selama periode tertentu. Untuk menghitung throughput yang diterima (byte per detik) untuk statistik apa pun, bagilah statistik dengan detik dalam periode yang ditentukan. Unit: Bita Statistik valid: `Sum`

Metrik	Deskripsi
`DataReadBytes`	Jumlah byte (jaringan I/O) dari dibaca oleh klien ke sistem file. `Sum`Statistik adalah jumlah total byte yang terkait dengan operasi baca selama periode yang ditentukan. Untuk menghitung throughput rata-rata (byte per detik) untuk suatu periode, bagilah `Sum` statistik dengan jumlah detik dalam periode yang ditentukan. Unit: Bita Statistik valid: `Sum`
`DataWriteBytes`	Jumlah byte (jaringan I/O) dari penulisan oleh klien ke sistem file. `Sum`Statistik adalah jumlah total byte yang terkait dengan operasi tulis selama periode yang ditentukan. Untuk menghitung throughput rata-rata (byte per detik) untuk suatu periode, bagilah `Sum` statistik dengan jumlah detik dalam periode yang ditentukan. Unit: Bita Statistik valid: `Sum`

Metrik	Deskripsi
`DataReadOperations`	Hitungan operasi baca (jaringan I/O) dari pembacaan oleh klien ke sistem file. `Sum`Statistik adalah jumlah total operasi I/O yang terjadi selama periode tertentu. Untuk menghitung operasi baca rata-rata per detik untuk suatu periode, bagilah `Sum` statistik dengan jumlah detik dalam periode yang ditentukan. Unit: Hitungan Statistik valid: `Sum`
`DataWriteOperations`	Hitungan operasi tulis (jaringan I/O) dari penulisan oleh klien ke sistem file. `Sum`Statistik adalah jumlah total operasi I/O yang terjadi selama periode tertentu. Untuk menghitung operasi tulis rata-rata per detik untuk suatu periode, bagilah `Sum` statistik dengan jumlah detik dalam periode yang ditentukan. Unit: Hitungan Statistik valid: `Sum`

Metrik	Deskripsi
`MetadataOperations`	Hitungan operasi metadata (jaringan I/O) oleh klien ke sistem file. `Sum`Statistik adalah jumlah total operasi I/O yang terjadi selama periode tertentu. Untuk menghitung rata-rata operasi metadata per detik untuk suatu periode, bagilah `Sum` statistik dengan jumlah detik dalam periode yang ditentukan. Unit: Hitungan Statistik valid: `Sum`
`DataReadOperationTime`	Jumlah total waktu yang dihabiskan dalam sistem file untuk operasi baca (jaringan I/O) dari klien yang mengakses data dalam sistem file. `Sum`Statistik adalah jumlah detik yang dihabiskan oleh operasi baca selama periode yang ditentukan. Untuk menghitung latensi baca rata-rata untuk suatu periode, bagilah `Sum` statistik dengan `DataReadOperations` metrik selama periode yang sama. `Sum` Unit: detik Statistik valid: `Sum`

Metrik	Deskripsi
DataWriteOperationTime	Jumlah total waktu yang dihabiskan dalam sistem file untuk memenuhi operasi tulis (jaringan I/O) dari klien yang mengakses data dalam sistem file. SumStatistik adalah jumlah detik yang dihabiskan oleh operasi tulis selama periode yang ditentukan. Untuk menghitung latensi tulis rata-rata untuk suatu periode, bagilah Sum statistik dengan DataWriteOperations metrik selama periode yang sama. Sum Unit: detik Statistik valid: Sum
CapacityPoolReadBytes	Jumlah byte yang dibaca (jaringan I/O) dari tingkat kumpulan kapasitas sistem file. Untuk memastikan integritas data, ONTAP melakukan operasi baca pada kumpulan kapasitas segera setelah melakukan operasi tulis. SumStatistik adalah jumlah total byte yang dibaca dari tingkat kumpulan kapasitas sistem file selama periode tertentu. Untuk menghitung byte kumpulan kapasitas per detik, bagi Sum statistik dengan detik dalam periode tertentu. Unit: Bita Statistik valid: Sum

Metrik	Deskripsi
`CapacityPoolReadOperations`	Jumlah operasi baca (jaringan I/O) dari tingkat kumpulan kapasitas sistem file. Ini berarti permintaan baca kumpulan kapasitas. Untuk memastikan integritas data, ONTAP melakukan operasi baca pada kumpulan kapasitas segera setelah melakukan operasi tulis. `Sum`Statistik adalah jumlah total operasi baca dari tingkat kumpulan kapasitas sistem file selama periode tertentu. Untuk menghitun g permintaan kumpulan kapasitas per detik, bagi `Sum` statistik dengan detik dalam periode tertentu. Unit: Hitungan Statistik valid: `Sum`
`CapacityPoolWriteBytes`	Jumlah byte yang ditulis (jaringan I/O) ke tingkat kumpulan kapasitas sistem file. Untuk memastikan integritas data, ONTAP melakukan operasi baca pada kumpulan kapasitas segera setelah melakukan operasi tulis. `Sum`Statistik adalah jumlah total byte yang ditulis ke tingkat kumpulan kapasitas sistem file selama periode tertentu. Untuk menghitun g byte kumpulan kapasitas per detik, bagi `Sum` statistik dengan detik dalam periode tertentu. Unit: Bita Statistik valid: `Sum`

Metrik	Deskripsi
`CapacityPoolWriteOperations`	Jumlah operasi tulis (jaringan I/O) ke sistem file dari tier pool kapasitas. Ini diterjemahkan menjadi permintaan tulis. Untuk memastikan integritas data, ONTAP melakukan operasi baca pada kumpulan kapasitas segera setelah melakukan operasi tulis. `Sum`Statistik adalah jumlah total operasi penulisan ke tingkat kumpulan kapasitas sistem file selama periode tertentu. Untuk menghitun g permintaan kumpulan kapasitas per detik, bagi `Sum` statistik dengan detik dalam periode tertentu. Unit: Hitungan Statistik valid: `Sum`

Metrik server file

Semua metrik ini mengambil satu dimensi,`FileSystemId`.

Metrik	Deskripsi
`CPUUtilization`	Persentase pemanfaatan sumber daya CPU sistem file. `Average`Statistik adalah pemanfaatan CPU rata-rata dari sistem file selama periode tertentu. `Minimum`Statistik adalah pemanfaatan CPU terendah dari sistem file selama periode tertentu.

Metrik	Deskripsi
	`Maximum`Statistik adalah pemanfaatan CPU tertinggi dari sistem file selama periode tertentu. Unit: Persen Statistik yang valid:`Average`,`Minimum`, dan `Maximum`
`FileServerDiskThroughputUtilization`	Throughput disk antara server file Anda dan tingkat utama, sebagai persentase dari batas yang disediakan ditentukan oleh kapasitas throughput. `Average`Statistik adalah persentase rata-rata pemanfaatan throughput disk server file selama periode tertentu. `Minimum`Statistik adalah persentase pemanfaatan terendah dari throughput disk server file selama periode tertentu. `Maximum`Statistik adalah pemanfaatan tertinggi dari throughput disk server file selama periode tertentu. Unit: Persen Statistik yang valid:`Average`,`Minimum`, dan `Maximum`

Metrik	Deskripsi
`FileServerDiskThroughputBalance`	Persentase kredit burst yang tersedia untuk throughput disk antara server file Anda dan tingkat utama. Ini berlaku untuk sistem file yang disediakan dengan kapasitas throughput 512 MBps atau kurang. `Average`Statistik adalah saldo burst rata-rata yang tersedia selama periode tertentu. `Minimum`Statistik adalah saldo burst minimum yang tersedia selama periode tertentu. `Maximum`Statistik adalah saldo burst maksimum yang tersedia selama periode tertentu. Unit: Persen Statistik yang valid:`Average`,`Minimum`, dan `Maximum`

Metrik	Deskripsi
`FileServerDiskIopsBalance`	Persentase kredit burst yang tersedia untuk IOPS disk antara server file Anda dan tingkat utama. Ini berlaku untuk sistem file yang disediakan dengan kapasitas throughput 512 MBps atau kurang. `Average`Statistik adalah saldo burst rata-rata yang tersedia selama periode tertentu. `Minimum`Statistik adalah saldo burst minimum yang tersedia selama periode tertentu. `Maximum`Statistik adalah saldo burst maksimum yang tersedia selama periode tertentu. Unit: Persen Statistik yang valid:`Average`,`Minimum`, dan `Maximum`

Metrik	Deskripsi
`FileServerDiskIopsUtilization`	Persentase pemanfaatan IOPS kapasitas IOPS disk yang tersedia untuk server file Anda. `Average`Statistik adalah pemanfaatan IOPS disk rata-rata dari sistem file selama periode tertentu. `Minimum`Statistik adalah pemanfaatan IOPS disk minimum dari sistem file selama periode tertentu. `Maximum`Statistik adalah pemanfaatan IOPS disk maksimum dari sistem file selama periode tertentu. Unit: Persen Statistik yang valid:`Average`,`Minimum`, dan `Maximum`

Metrik	Deskripsi
`FileServerCacheHitRatio`	Persentase semua permintaan baca yang dilayani oleh data dalam RAM sistem file dan cache NVMe. Persentase yang lebih tinggi berarti bahwa lebih banyak pembacaan disajikan oleh cache baca sistem file. Unit: Persen `Average`Statistik adalah persentase hit cache rata-rata untuk sistem file selama periode tertentu. `Minimum`Statistik adalah persentase hit cache terendah untuk sistem file selama periode tertentu. `Maximum`Statistik adalah persentase hit cache tertinggi untuk sistem file selama periode tertentu. Statistik yang valid:`Average`,`Minimum`, dan `Maximum`

Metrik I/O disk

Semua metrik ini mengambil satu dimensi,`FileSystemId`.

Metrik	Deskripsi
`DiskReadBytes`	Jumlah byte (disk I/O) dari disk apa pun dibaca ke tingkat utama sistem file. `Sum`Statistik adalah jumlah total byte yang dibaca dari sistem file selama periode tertentu.

Metrik	Deskripsi
	Untuk menghitung throughput disk baca (byte per detik) untuk statistik apa pun, bagilah `Sum` statistik dengan detik dalam periode yang ditentukan. Unit: Bita Statistik valid: `Sum`
`DiskWriteBytes`	Jumlah byte (disk I/O) dari disk apa pun menulis ke tingkat utama sistem file. `Sum`Statistik adalah jumlah total byte yang ditulis dari sistem file selama periode tertentu. Untuk menghitung throughput disk tulis (byte per detik) untuk statistik apa pun, bagilah `Sum` statistik dengan detik dalam periode yang ditentukan. Unit: Bita Statistik valid: `Sum`

Metrik	Deskripsi
`DiskIopsUtilization`	Disk IOPS antara server file Anda dan volume penyimpanan, sebagai persentase dari batas IOPS disk yang disediakan tingkat primer. `Average`Statistik adalah pemanfaatan IOPS disk rata-rata dari sistem file selama periode tertentu. `Minimum`Statistik adalah pemanfaatan IOPS disk minimum dari sistem file selama periode tertentu. `Maximum`Statistik adalah pemanfaatan IOPS disk maksimum dari sistem file selama periode tertentu. Unit: Persen Statistik yang valid:`Average`,`Minimum`, dan `Maximum`
`DiskReadOperations`	Jumlah operasi baca (disk I/O) dari tingkat utama sistem file. `Sum`Statistik adalah jumlah total operasi baca dari tingkat primer selama periode tertentu. Unit: Hitungan Statistik valid: `Sum`

Metrik	Deskripsi
DiskWriteOperations	Jumlah operasi tulis (disk I/O) ke tingkat utama sistem file. SumStatistik adalah jumlah total operasi penulisan ke tingkat primer selama periode tertentu. Unit: Hitungan Statistik valid: Sum

Metrik kapasitas penyimpanan

Semua metrik ini mengambil satu dimensi,FileSystemId.

Metrik	Deskripsi
StorageEfficiencySavings	Byte disimpan dari fitur efisiensi penyimpanan (kompresi, deduplikasi, dan pemadatan). AverageStatistik adalah penghematan efisiensi penyimpanan rata-rata selama periode tertentu. Untuk menghitung penghematan efisiensi penyimpanan sebagai persentase dari semua data yang disimpan, selama periode satu menit, bagi StorageEfficiencyS avings dengan jumlah StorageEf ficiencySavings dan metrik sistem StorageUsed file, menggunakan Sum statistik untukStorageUsed . MinimumStatistik adalah penghematan efisiensi penyimpanan minimum selama periode tertentu.

Metrik	Deskripsi
	`Maximum`Statistik adalah penghematan efisiensi penyimpanan maksimum selama periode tertentu. Unit: Bita Statistik yang valid:`Average`,`Minimum`, dan `Maximum`
`StorageUsed`	Jumlah total data fisik yang tersimpan pada sistem file, pada tingkat primer (SSD) dan tingkat kolam kapasitas. Metrik ini mencakup penghematan dari fitur efisiensi penyimpanan, seperti kompresi data dan deduplikasi. Unit: Bita Statistik yang valid:`Average`,`Minimum`, dan `Maximum`

Metrik	Deskripsi
`LogicalDataStored`	Jumlah total data logis yang disimpan pada sistem file, mengingat tingkat SSD dan tingkat kolam kapasitas. Metrik ini mencakup ukuran logis total snapshot dan FlexClones, tetapi tidak termasuk penghematan efisiensi penyimpanan yang dicapai melalui kompresi, pemadatan, dan deduplikasi. Untuk menghitung penghematan efisiensi penyimpanan dalam byte, ambil `Average` dari `StorageUsed` selama periode tertentu dan kurangi dari periode yang sama`Average`. `LogicalDataStored` Untuk menghitung penghematan efisiensi penyimpanan sebagai persentase dari total ukuran data logis, ambil `Average` dari `StorageUsed` selama periode tertentu dan kurangi dari `LogicalDataStored` periode yang sama`Average`. Kemudian bagi perbedaannya `Average` dengan `LogicalDataStored` periode yang sama. Unit: Bita Statistik yang valid:`Average`,`Minimum`, dan `Maximum`

Metrik sistem file terperinci

Metrik sistem file terperinci adalah metrik pemanfaatan penyimpanan terperinci untuk setiap tingkatan penyimpanan Anda. Metrik sistem file terperinci semuanya memiliki dimensi`FileSystemId`,`StorageTier`, dan`DataType`.

- `StorageTier`Dimensi menunjukkan tingkat penyimpanan yang diukur metrik, dengan kemungkinan nilai `SSD` dan`StandardCapacityPool`.

- `DataType`Dimensi menunjukkan jenis data yang diukur metrik, dengan nilai yang mungkin`All`.

Ada baris untuk setiap kombinasi unik dari pasangan nilai kunci metrik dan dimensi tertentu, dengan deskripsi tentang apa yang diukur kombinasi itu.

Metrik	Deskripsi
`StorageCapacityUtilization`	Pemanfaatan kapasitas penyimpanan untuk setiap agregat sistem file Anda. Ada satu metrik yang dipancarkan setiap menit untuk setiap agregat sistem file Anda. `Average`Statistik adalah jumlah rata-rata pemanfaatan kapasitas penyimpanan untuk tingkat kinerja sistem file Anda selama periode yang ditentukan. `Minimum`Statistik adalah jumlah pemanfaatan kapasitas penyimpanan terendah untuk tingkat kinerja sistem file Anda selama periode yang ditentukan. `Maximum`Statistik adalah jumlah pemanfaatan kapasitas penyimpanan tertinggi untuk tingkat kinerja sistem file Anda selama periode yang ditentukan. Unit: Persen Statistik yang valid:`Average`,`Minimum`, dan `Maximum`
`StorageCapacity`	Total kapasitas penyimpanan tingkat primer (SSD). Unit: Bita Statistik valid: `Maximum`

Metrik	Deskripsi
`StorageUsed`	Kapasitas penyimpanan fisik yang digunakan dalam byte, khusus untuk tingkat penyimpan an. Nilai ini mencakup penghematan dari fitur efisiensi penyimpanan, seperti kompresi data dan deduplikasi. Nilai dimensi yang valid untuk `StorageTier` are `SSD` dan`StandardC apacityPool` , sesuai dengan tingkat penyimpanan yang diukur metrik ini. Metrik ini juga membutuhkan `DataType` dimensi dengan nilai`All`. The`Average`,`Minimum`, dan `Maximum` statistik adalah konsumsi penyimpanan per tingkat dalam byte untuk periode tertentu. Untuk menghitung pemanfaatan kapasitas penyimpanan tingkat penyimpanan utama (SSD) Anda, bagilah salah satu statistik ini dengan `Maximum` `StorageCapacity` periode yang sama, dengan `StorageTier` dimensi yang sama dengan. `SSD` Untuk menghitung kapasitas penyimpanan gratis tingkat penyimpanan utama (SSD) Anda dalam byte, kurangi salah satu statistik ini dari periode yang sama, dengan dimensi yang `StorageTier` sama dengan. `Maximum` `StorageCapacity` `SSD` Unit: Bita Statistik yang valid:`Average`,`Minimum`, dan `Maximum`

Metrik sistem file scale-out

Metrik berikut disediakan untuk FSx untuk sistem file ONTAP dengan dua atau lebih pasangan ketersediaan tinggi (HA). Untuk metrik, titik data dipancarkan untuk setiap pasangan HA dan untuk setiap agregat (untuk metrik pemanfaatan penyimpanan).

> **Note**
>
> Jika Anda memiliki sistem file dengan beberapa pasangan HA, Anda juga dapat menggunakan metrik sistem file pasangan HA tunggal dan metrik volume.

Topik

Metrik I/O jaringan

Semua metrik ini mengambil dua dimensi, `FileSystemId` dan`FileServer`.

- `FileSystemId`— ID AWS sumber daya sistem file Anda.
- `FileServer`— Nama server file (atau node) di ONTAP (misalnya,`FsxId01234567890abcdef-01`). Server file bernomor ganjil adalah server file yang disukai (yaitu, mereka melayani lalu lintas kecuali sistem file gagal ke server file sekunder), sedangkan server file bernomor genap adalah server file sekunder (yaitu, mereka melayani lalu lintas hanya ketika mitra mereka tidak tersedia). Karena itu, server file sekunder biasanya menunjukkan pemanfaatan yang lebih sedikit daripada server file pilihan.

Metrik	Deskripsi
`NetworkThroughputUtilization`	Pemanfaatan throughput jaringan sebagai persentase dari throughput jaringan yang tersedia untuk sistem file Anda. Metrik ini setara dengan maksimum `NetworkSe`

Metrik	Deskripsi
	`ntBytes` dan `NetworkReceivedBytes` sebagai persentase kapasitas throughput jaringan dari satu pasangan HA untuk sistem file Anda. Semua lalu lintas dipertimbangkan dalam metrik ini, termasuk tugas latar belakang (seperti SnapMirror, tiering, dan backup). Ada satu metrik yang dipancarkan setiap menit untuk setiap server file sistem file Anda. `Average`Statistik adalah pemanfaatan throughput jaringan rata-rata untuk server file yang diberikan selama periode yang ditentukan. `Minimum`Statistik adalah pemanfaatan throughput jaringan terendah untuk server file yang diberikan selama satu menit, untuk periode yang ditentukan. `Maximum`Statistik adalah pemanfaatan throughput jaringan tertinggi untuk server file yang diberikan selama satu menit, untuk periode yang ditentukan. Unit: Persen Statistik yang valid:`Average`,`Minimum`, dan `Maximum`

Metrik	Deskripsi
`NetworkSentBytes`	Jumlah byte (jaringan IO) yang dikirim oleh sistem file Anda. Semua lalu lintas dipertimb angkan dalam metrik ini, termasuk tugas latar belakang (seperti SnapMirror, tiering, dan backup). Ada satu metrik yang dipancarkan setiap menit untuk setiap server file sistem file Anda. `Sum`Statistik adalah jumlah total byte yang dikirim melalui jaringan oleh server file yang diberikan selama periode yang ditentukan. `Average`Statistik adalah jumlah rata-rata byte yang dikirim melalui jaringan oleh server file yang diberikan selama periode yang ditentuka n. `Minimum`Statistik adalah jumlah byte terendah yang dikirim melalui jaringan oleh server file yang diberikan selama periode yang ditentuka n. `Maximum`Statistik adalah jumlah byte tertinggi yang dikirim melalui jaringan oleh server file yang diberikan selama periode yang ditentuka n. Untuk menghitung throughput terkirim (byte per detik) untuk statistik apa pun, bagilah statistik dengan detik dalam periode yang ditentukan. Unit: Bita Statistik yang valid:`Sum`,`Average`,`Minimum`, dan `Maximum`

Metrik	Deskripsi
`NetworkReceivedBytes`	Jumlah byte (jaringan IO) yang diterima oleh sistem file Anda. Semua lalu lintas dipertimb angkan dalam metrik ini, termasuk tugas latar belakang (seperti SnapMirror, tiering, dan backup). Ada satu metrik yang dipancarkan setiap menit untuk setiap server file sistem file Anda. `Sum`Statistik adalah jumlah total byte yang diterima melalui jaringan oleh server file yang diberikan selama periode yang ditentukan. `Average`Statistik adalah jumlah rata-rata byte yang diterima melalui jaringan oleh server file yang diberikan setiap menit selama periode yang ditentukan. `Minimum`Statistik adalah jumlah byte terendah yang diterima melalui jaringan oleh server file yang diberikan setiap menit selama periode yang ditentukan. `Maximum`Statistik adalah jumlah byte tertinggi yang diterima melalui jaringan oleh server file yang diberikan setiap menit selama periode yang ditentukan. Untuk menghitung throughput yang diterima (byte per detik) untuk statistik apa pun, bagilah statistik dengan detik dalam periode tersebut. Unit: Bita Statistik yang valid:`Sum`,`Average`,`Minimum`, dan `Maximum`

Metrik server file

Semua metrik ini mengambil dua dimensi, `FileSystemId` dan`FileServer`.

Metrik	Deskripsi
`CPUUtilization`	Persentase pemanfaatan sumber daya CPU sistem file. Ada satu metrik yang dipancarkan setiap menit untuk setiap server file sistem file Anda. `Average`Statistik adalah pemanfaatan CPU rata-rata dari sistem file selama periode tertentu. `Minimum`Statistik adalah pemanfaatan CPU terendah untuk server file yang diberikan selama periode yang ditentukan. `Maximum`Statistik adalah pemanfaatan CPU tertinggi untuk server file yang diberikan selama periode yang ditentukan. Unit: Persen Statistik yang valid:`Average`,`Minimum`, dan `Maximum`
`FileServerDiskThroughputUtilization`	Throughput disk antara server file Anda dan agregat, sebagai persentase dari batas yang disediakan ditentukan oleh kapasitas throughput. Semua lalu lintas dipertimbangkan dalam metrik ini, termasuk tugas latar belakang (seperti SnapMirror, tiering, dan backup). Metrik ini setara dengan jumlah `DiskReadBytes` dan `DiskWriteBytes` sebagai persentase kapasitas throughput disk server file dari satu pasangan HA untuk sistem file Anda. Ada satu

Metrik	Deskripsi
	metrik yang dipancarkan setiap menit untuk setiap server file sistem file Anda. `Average`Statistik adalah rata-rata pemanfaat an throughput disk server file untuk server file yang diberikan selama periode yang ditentuka n. `Minimum`Statistik adalah pemanfaatan throughput disk server file terendah untuk server file yang diberikan selama periode yang ditentukan. `Maximum`Statistik adalah pemanfaatan throughput disk server file tertinggi untuk server file yang diberikan selama periode yang ditentukan. Unit: Persen Statistik yang valid:`Average`,`Minimum`, dan `Maximum`

Metrik	Deskripsi
`FileServerDiskIopsUtilization`	Pemanfaatan IOPS kapasitas IOPS disk yang tersedia untuk server file Anda, sebagai persentase dari batas IOPS disk. Ini berbeda dari `DiskIopsUtilization` penggunaan IOPS disk dari maksimum yang dapat ditangani oleh server file Anda, dibandingkan dengan IOPS disk yang disediakan. Semua lalu lintas dipertimbangkan dalam metrik ini, termasuk tugas latar belakang (seperti SnapMirror, tiering, dan backup). Ada satu metrik yang dipancarkan setiap menit untuk setiap server file sistem file Anda. `Average`Statistik adalah pemanfaatan IOPS disk rata-rata untuk server file yang diberikan selama periode yang ditentukan. `Minimum`Statistik adalah pemanfaatan IOPS disk terendah untuk server file yang diberikan selama periode yang ditentukan. `Maximum`Statistik adalah pemanfaatan IOPS disk tertinggi untuk server file yang diberikan selama periode yang ditentukan. Unit: Persen Statistik yang valid:`Average`,`Minimum`, dan `Maximum`

Metrik	Deskripsi
`FileServerCacheHitRatio`	Persentase semua permintaan baca yang dilayani oleh data yang berada di RAM sistem file atau cache NVMe untuk masing-masing pasangan HA Anda (misalnya, server file aktif dalam pasangan HA). Persentase yang lebih tinggi menunjukkan rasio pembacaan cache yang lebih tinggi terhadap total pembacaan. Semua I/O dipertimbangkan, termasuk tugas latar belakang (seperti SnapMirror, tiering, dan backup). Ada satu metrik yang dipancarkan setiap menit untuk setiap server file sistem file Anda. Unit: Persen `Average`Statistik adalah rasio hit cache rata-rata untuk salah satu pasangan HA sistem file Anda selama periode yang ditentukan. `Minimum`Statistik adalah rasio hit cache terendah untuk salah satu pasangan HA sistem file Anda selama periode yang ditentukan. `Maximum`Statistik adalah rasio hit cache tertinggi untuk salah satu pasangan HA sistem file Anda selama periode yang ditentukan. Statistik yang valid:`Average`,`Minimum`, dan `Maximum`

Metrik I/O disk

Semua metrik ini mengambil dua dimensi, `FileSystemId` dan`Aggregate`.

- `FileSystemId`— ID AWS sumber daya sistem file Anda.

- `Aggregate`— Tingkat kinerja sistem file Anda terdiri dari beberapa kumpulan penyimpanan yang disebut agregat. Ada satu agregat untuk setiap pasangan HA. Misalnya, agregat `aggr1` peta ke server file `FsxId01234567890abcdef-01` (server file aktif) dan server file `FsxId01234567890abcdef-02` (server file sekunder) dalam pasangan HA.

Metrik	Deskripsi
`DiskReadBytes`	Jumlah byte (disk IO) dari disk ay dibaca dari agregat ini. Semua lalu lintas dipertimbangkan dalam metrik ini, termasuk tugas latar belakang (seperti SnapMirror, tiering, dan backup). Ada satu metrik yang dipancarkan setiap menit untuk setiap agregat sistem file Anda. `Sum`Statistik adalah jumlah total byte yang dibaca setiap menit dari agregat yang diberikan selama periode yang ditentukan. `Average`Statistik adalah jumlah rata-rata byte yang dibaca setiap menit dari agregat yang diberikan selama periode yang ditentukan. `Minimum`Statistik adalah jumlah byte terendah yang dibaca setiap menit dari agregat yang diberikan selama periode yang ditentukan. `Maximum`Statistik adalah jumlah byte tertinggi yang dibaca setiap menit dari agregat yang diberikan selama periode yang ditentukan. Untuk menghitung throughput disk baca (byte per detik) untuk statistik apa pun, bagilah statistik dengan detik dalam periode tersebut. Unit: Bita Statistik yang valid:`Sum`,`Average`,`Minimum`, dan `Maximum`

Metrik	Deskripsi
`DiskWriteBytes`	Jumlah byte (disk IO) dari disk apa pun menulis ke agregat ini. Semua lalu lintas dipertimb angkan dalam metrik ini, termasuk tugas latar belakang (seperti SnapMirror, tiering, dan backup). Ada satu metrik yang dipancarkan setiap menit untuk setiap agregat sistem file Anda. `Sum`Statistik adalah jumlah total byte yang ditulis ke agregat yang diberikan selama periode yang ditentukan. `Average`Statistik adalah jumlah rata-rata byte yang ditulis ke agregat yang diberikan setiap menit selama periode yang ditentukan. `Minimum`Statistik adalah jumlah byte terendah yang ditulis ke agregat yang diberikan setiap menit selama periode yang ditentukan. `Maximum`Statistik adalah jumlah byte tertinggi yang ditulis ke agregat yang diberikan setiap menit selama periode yang ditentukan. Untuk menghitung throughput disk tulis (byte per detik) untuk statistik apa pun, bagilah statistik dengan detik dalam periode yang ditentukan. Unit: Bita Statistik yang valid:`Sum`,`Average`,`Minimum`, dan `Maximum`

Metrik	Deskripsi
`DiskIopsUtilization`	Pemanfaatan IOPS disk dari satu agregat, sebagai persentase dari batas IOPS disk agregat (yaitu, total IOPS sistem file dibagi dengan jumlah pasangan HA untuk sistem file Anda). Ini berbeda dari `FileServerDiskIopsUtilization` itu adalah pemanfaatan IOPS disk yang disediakan terhadap batas IOPS yang Anda berikan, sebagai lawan dari IOPS disk maksimum yang didukung oleh server file (yaitu, ditentukan oleh kapasitas throughput Anda yang dikonfigurasi per pasangan HA). Semua lalu lintas dipertimbangkan dalam metrik ini, termasuk tugas latar belakang (seperti SnapMirror, tiering, dan backup). Ada satu metrik yang dipancarkan setiap menit untuk setiap agregat sistem file Anda. `Average`Statistik adalah pemanfaatan IOPS disk rata-rata untuk agregat yang diberikan selama periode yang ditentukan. `Minimum`Statistik adalah pemanfaatan IOPS disk terendah untuk agregat yang diberikan selama periode yang ditentukan. `Maximum`Statistik ii pemanfaatan IOPS disk tertinggi untuk agregat yang diberikan selama periode yang ditentukan. Unit: Persen Statistik yang valid:`Average`,`Minimum`, dan `Maximum`

Metrik	Deskripsi
`DiskReadOperations`	Jumlah operasi baca (disk IO) ke agregat ini. Semua lalu lintas dipertimbangkan dalam metrik ini, termasuk tugas latar belakang (seperti SnapMirror, tiering, dan backup). Ada satu metrik yang dipancarkan setiap menit untuk setiap agregat sistem file Anda. `Sum`Statistik adalah jumlah total operasi baca yang dilakukan oleh agregat yang diberikan selama periode yang ditentukan. `Average`Statistik adalah jumlah rata-rata operasi baca yang dilakukan setiap menit oleh agregat yang diberikan selama periode yang ditentukan. `Minimum`Statistik adalah jumlah operasi baca terendah yang dilakukan setiap menit oleh agregat yang diberikan selama periode yang ditentukan. `Maximum`Statistik adalah jumlah operasi baca tertinggi yang dilakukan setiap menit oleh agregat yang diberikan selama periode yang ditentukan. Untuk menghitung IOPS disk rata-rata selama periode tersebut, gunakan `Average` statistik dan bagi hasilnya dengan 60 (detik). Unit: Hitungan Statistik yang valid:`Sum`,`Average`,`Minimum`, dan `Maximum`

Metrik	Deskripsi
`DiskWriteOperations`	Jumlah operasi tulis (disk IO) ke agregat ini. Semua lalu lintas dipertimbangkan dalam metrik ini, termasuk tugas latar belakang (seperti SnapMirror, tiering, dan backup). Ada satu metrik yang dipancarkan setiap menit untuk setiap agregat sistem file Anda. `Sum`Statistik adalah jumlah total operasi penulisan yang dilakukan oleh agregat yang diberikan selama periode yang ditentukan. `Average`Statistik adalah jumlah rata-rata operasi tulis yang dilakukan setiap menit oleh agregat yang diberikan selama periode yang ditentukan. Untuk menghitung IOPS disk rata-rata selama periode tersebut, gunakan `Average` statistik dan bagi hasilnya dengan 60 (detik). Unit: Hitungan Statistik yang valid: `Sum` dan `Average`

Metrik sistem file terperinci

Metrik sistem file terperinci adalah metrik pemanfaatan penyimpanan terperinci untuk setiap tingkatan penyimpanan Anda. Metrik sistem file terperinci memiliki`FileSystemId`,`StorageTier`, dan `DataType` dimensi, atau,`FileSystemId`, `StorageTierDataType`, dan `Aggregate` dimensi.

- Ketika `Aggregate` dimensi tidak disediakan, metrik adalah untuk seluruh sistem file Anda. `StorageCapacity`Metrik `StorageUsed` dan memiliki titik data tunggal setiap menit yang sesuai dengan total penyimpanan yang dikonsumsi sistem file (per tingkat penyimpanan) dan kapasitas penyimpanan total (untuk tingkat SSD). Sementara itu, `StorageCapacityUtilization` metrik memancarkan satu metrik setiap menit untuk setiap agregat.
- Ketika `Aggregate` dimensi disediakan, metrik untuk setiap agregat.

Arti dimensi adalah sebagai berikut:

- `FileSystemId`— ID AWS sumber daya sistem file Anda.
- `Aggregate`— Tingkat kinerja sistem file Anda terdiri dari beberapa kumpulan penyimpanan yang disebut agregat. Ada satu agregat untuk setiap pasangan HA. Misalnya, agregat `aggr1` peta ke server file `FsxId01234567890abcdef-01` (server file aktif) dan server file `FsxId01234567890abcdef-02` (server file sekunder) dalam pasangan HA.
- `StorageTier`— Menunjukkan tingkat penyimpanan yang diukur metrik, dengan kemungkinan nilai `SSD` dan`StandardCapacityPool`.
- `DataType`— Menunjukkan jenis data yang diukur metrik, dengan nilai yang mungkin`All`.

Ada baris untuk setiap kombinasi unik dari pasangan nilai kunci metrik dan dimensi tertentu, dengan deskripsi tentang apa yang diukur kombinasi itu.

Metrik	Deskripsi
`StorageCapacityUtilization`	Pemanfaatan kapasitas penyimpanan untuk agregat sistem file tertentu. Ada satu metrik yang dipancarkan setiap menit untuk setiap agregat sistem file Anda. `Average`Statistik adalah jumlah rata-rata pemanfaatan kapasitas penyimpanan untuk agregat tertentu selama periode yang ditentuka n. `Minimum`Statistik adalah jumlah minimum pemanfaatan kapasitas penyimpanan untuk agregat tertentu selama periode yang ditentuka n. `Maximum`Statistik adalah jumlah maksimum pemanfaatan kapasitas penyimpanan untuk agregat tertentu selama periode yang ditentuka n. Unit: Persen

Metrik	Deskripsi
	Statistik yang valid:`Average`,`Minimum`, dan `Maximum`
`StorageCapacity`	Kapasitas penyimpanan untuk agregat sistem file tertentu. Ada satu metrik yang dipancark an setiap menit untuk setiap agregat sistem file Anda. `Average`Statistik adalah jumlah rata-rata kapasitas penyimpanan untuk agregat tertentu selama periode yang ditentukan. `Minimum`Statistik adalah jumlah minimum kapasitas penyimpanan untuk agregat tertentu selama periode yang ditentukan. `Maximum`Statistik adalah jumlah maksimum kapasitas penyimpanan untuk agregat tertentu selama periode yang ditentukan. Unit: Bita Statistik yang valid:`Average`,`Minimum`, dan `Maximum`

Metrik	Deskripsi
`StorageUsed`	Kapasitas penyimpanan fisik yang digunakan dalam byte, khusus untuk tingkat penyimpan an. Nilai ini mencakup penghematan dari fitur efisiensi penyimpanan, seperti kompresi data dan deduplikasi. Nilai dimensi yang valid untuk `StorageTier` are `SSD` dan`StandardC apacityPool` , sesuai dengan tingkat penyimpanan yang diukur metrik ini. Ada satu metrik yang dipancarkan setiap menit untuk setiap agregat sistem file Anda. `Average`Statistik adalah jumlah rata-rata kapasitas penyimpanan fisik yang dikonsumsi pada tingkat penyimpanan yang diberikan oleh agregat yang diberikan selama periode yang ditentukan. `Minimum`Statistik adalah jumlah minimum kapasitas penyimpanan fisik yang dikonsumsi pada tingkat penyimpanan yang diberikan oleh agregat yang diberikan selama periode yang ditentukan. `Maximum`Statistik adalah jumlah maksimum kapasitas penyimpanan fisik yang dikonsumsi pada tingkat penyimpanan yang diberikan oleh agregat yang diberikan selama periode yang ditentukan. Unit: Bita Statistik yang valid:`Average`,`Minimum`, dan `Maximum`

Metrik volume

Amazon fsX untuk sistem file NetApp ONTAP Anda dapat memiliki satu atau lebih volume yang menyimpan data Anda. Masing-masing volume ini memiliki satu set metrik, diklasifikasikan sebagai Metrik volume atau metrik volume terperinci.

- Metrik volume adalah metrik kinerja per volume dan penyimpanan yang mengambil dua dimensi, dan. `FileSystemId` `VolumeId` `FileSystemId`memetakan ke sistem file yang menjadi milik volume.
- Metrik volume terperinci adalah per-storage-tier metrik yang mengukur konsumsi penyimpanan per tingkat dengan `StorageTier` dimensi (dengan kemungkinan nilai `SSD` dan`StandardCapacityPool`) dan per tipe data dengan `DataType` dimensi (dengan kemungkinan nilai`User`,`Snapshot`, dan`Other`). Metrik ini memiliki`FileSystemId`,, `VolumeId``StorageTier`, dan `DataType` dimensi.

Topik

Metrik I/O jaringan

Semua metrik ini mengambil dua dimensi, `FileSystemId` dan`VolumeId`.

Metrik	Deskripsi
`DataReadBytes`	Jumlah byte (jaringan I/O) dibaca dari volume oleh klien. `Sum`Statistik adalah jumlah total byte yang terkait dengan operasi baca selama periode yang ditentukan. Untuk menghitung throughpu t rata-rata (byte per detik) untuk suatu periode, bagilah `Sum` statistik dengan jumlah detik dalam periode yang ditentukan. Unit: Bita

Metrik	Deskripsi
	Statistik valid: `Sum`
`DataWriteBytes`	Jumlah byte (jaringan I/O) yang ditulis ke volume oleh klien. `Sum`Statistik adalah jumlah total byte yang terkait dengan operasi tulis selama periode yang ditentukan. Untuk menghitung throughput rata-rata (byte per detik) untuk suatu periode, bagilah `Sum` statistik dengan jumlah detik dalam periode yang ditentukan. Unit: Bita Statistik valid: `Sum`
`DataReadOperations`	Jumlah operasi baca (jaringan I/O) pada volume oleh klien. `Sum`Statistik adalah jumlah total operasi baca selama periode yang ditentukan. Untuk menghitung operasi baca rata-rata per detik untuk suatu periode, bagilah `Sum` statistik dengan jumlah detik dalam periode yang ditentukan. Unit: Hitungan Statistik valid: `Sum`

Metrik	Deskripsi
`DataWriteOperations`	Jumlah operasi tulis (jaringan I/O) pada volume oleh klien. `Sum`Statistik adalah jumlah total operasi penulisan selama periode yang ditentukan. Untuk menghitung operasi tulis rata-rata per detik untuk suatu periode, bagilah `Sum` statistik dengan jumlah detik dalam periode yang ditentukan. Unit: Hitungan Statistik valid: `Sum`
`MetadataOperations`	Jumlah operasi I/O (jaringan I/O) dari aktivitas metadata oleh klien ke volume. `Sum`Statistik adalah jumlah total operasi metadata selama periode yang ditentukan. Untuk menghitung rata-rata operasi metadata per detik untuk suatu periode, bagilah `Sum` statistik dengan jumlah detik dalam periode yang ditentukan. Unit: Hitungan Statistik valid: `Sum`

Metrik	Deskripsi
DataReadOperationTime	Jumlah total waktu yang dihabiskan dalam volume untuk operasi baca (jaringan I/O) dari klien yang mengakses data dalam volume. SumStatistik adalah jumlah detik yang dihabiskan oleh operasi baca selama periode yang ditentukan. Untuk menghitung latensi baca rata-rata untuk suatu periode, bagilah Sum statistik dengan DataReadOperations metrik selama periode yang sama. Sum Unit: detik Statistik valid: Sum
DataWriteOperationTime	Jumlah total waktu yang dihabiskan dalam volume untuk memenuhi operasi tulis (jaringan I/O) dari klien yang mengakses data dalam volume. SumStatistik adalah jumlah detik yang dihabiskan oleh operasi tulis selama periode yang ditentukan. Untuk menghitung latensi tulis rata-rata untuk suatu periode, bagilah Sum statistik dengan DataWriteOperations metrik selama periode yang sama. Sum Unit: detik Statistik valid: Sum

Metrik	Deskripsi
`MetadataOperationTime`	Jumlah total waktu yang dihabiskan dalam volume untuk memenuhi operasi metadata (jaringan I/O) dari klien yang mengakses data dalam volume. `Sum`Statistik adalah jumlah detik yang dihabiskan oleh operasi baca selama periode yang ditentukan. Untuk menghitung latensi rata-rata untuk suatu periode, bagilah `Sum` statistik dengan `MetadataOperations` periode yang sama. `Sum` Unit: detik Statistik valid: `Sum`
`CapacityPoolReadBytes`	Jumlah byte yang dibaca (jaringan I/O) dari tingkat kumpulan kapasitas volume. Untuk memastikan integritas data, ONTAP melakukan operasi baca pada kumpulan kapasitas segera setelah melakukan operasi tulis. `Sum`Statistik adalah jumlah total byte yang dibaca dari tingkat kumpulan kapasitas volume selama periode tertentu. Untuk menghitung byte kumpulan kapasitas per detik, bagi `Sum` statistik dengan detik dalam periode tertentu. Unit: Bita Statistik valid: `Sum`

Metrik	Deskripsi
`CapacityPoolReadOperations`	Jumlah operasi baca (jaringan I/O) dari tingkat kumpulan kapasitas volume. Ini berarti permintaan baca kumpulan kapasitas. Untuk memastikan integritas data, ONTAP melakukan operasi baca pada kumpulan kapasitas segera setelah melakukan operasi tulis. `Sum`Statistik adalah jumlah total operasi baca dari tingkat kumpulan kapasitas volume selama periode tertentu. Untuk menghitung permintaan kumpulan kapasitas per detik, bagi `Sum` statistik dengan detik dalam periode tertentu. Unit: Hitungan Statistik valid: `Sum`
`CapacityPoolWriteBytes`	Jumlah byte yang ditulis (jaringan I/O) ke tingkat kumpulan kapasitas volume. Untuk memastikan integritas data, ONTAP melakukan operasi baca pada kumpulan kapasitas segera setelah melakukan operasi tulis. `Sum`Statistik adalah jumlah total byte yang ditulis ke tingkat kumpulan kapasitas volume selama periode tertentu. Untuk menghitung byte kumpulan kapasitas per detik, bagi `Sum` statistik dengan detik dalam periode tertentu. Unit: Bita Statistik valid: `Sum`

Metrik	Deskripsi
`CapacityPoolWriteOperations`	Jumlah operasi tulis (jaringan I/O) ke volume dari tier pool kapasitas. Ini diterjemahkan menjadi permintaan tulis. Untuk memastikan integritas data, ONTAP melakukan operasi baca pada kumpulan kapasitas segera setelah melakukan operasi tulis. `Sum`Statistik adalah jumlah total operasi tulis ke tingkat kumpulan kapasitas volume selama periode tertentu. Untuk menghitung permintaan kumpulan kapasitas per detik, bagi `Sum` statistik dengan detik dalam periode tertentu. Unit: Hitungan Statistik valid: `Sum`

Metrik kapasitas penyimpanan

Semua metrik ini mengambil dua dimensi, `FileSystemId` dan`VolumeId`.

Metrik	Deskripsi
`StorageCapacity`	Ukuran volume dalam byte. Unit: Bita Statistik valid: `Maximum`
`StorageUsed`	Kapasitas penyimpanan logis yang digunakan dari volume. Unit: Bita

Metrik	Deskripsi
	Statistik yang valid:`Average`,`Minimum`, dan `Maximum`
`StorageCapacityUtilization`	Pemanfaatan kapasitas penyimpanan volume. Unit: Persen Statistik valid: `Average`
`FilesUsed`	File yang digunakan (jumlah file atau inode) pada volume. Unit: Hitungan Statistik yang valid:`Average`,`Minimum`, dan `Maximum`
`FilesCapacity`	Jumlah total inode yang dapat dibuat pada volume. Unit: Hitungan Statistik valid: `Maximum`

Metrik volume terperinci

Metrik volume terperinci membutuhkan lebih banyak dimensi daripada metrik volume, memungkinkan pengukuran data Anda yang lebih terperinci. Semua metrik volume rinci memiliki dimensi`FileSystemId`,, `VolumeId``StorageTier`, dan`DataType`.

- `StorageTier`Dimensi menunjukkan tingkat penyimpanan yang diukur metrik, dengan kemungkinan nilai`All`,`SSD`, dan`StandardCapacityPool`.
- `DataType`Dimensi menunjukkan jenis data yang diukur metrik, dengan kemungkinan nilai`All`,`User`,`Snapshot`, dan`Other`.

Tabel berikut mendefinisikan apa ukuran `StorageUsed` metrik untuk dimensi yang terdaftar.

Metrik	Deskripsi
`StorageUsed`	Jumlah ruang logis yang digunakan, dalam byte. Metrik ini mengukur berbagai jenis konsumsi ruang tergantung pada dimensi yang digunakan dengan metrik ini. Saat menyetel `StorageTier` ke `SSD` atau`StandardCapacityPool`, dan menyetel `DataType` ke`All`, metrik ini mengukur penggunaan ruang logis untuk volume ini untuk SSD dan tingkatan kumpulan kapasitas Anda. Saat menyetel `DataType` dimensi ke `UserSnapshot`,`Other`, atau, dan pengaturan `StorageTier` ke`All`, metrik ini mengukur penggunaan ruang logis untuk setiap jenis data masing-masing. Konsumsi `Snapshot` data mencakup cadangan snapshot, yang merupakan 5% dari ukuran volume secara default. Unit: Bita Statistik yang valid:`Average`,`Minimum`, dan `Maximum`
`StorageCapacityUtilization`	Persentase ruang disk fisik yang digunakan volume. Unit: Persen Statistik valid: `Maximum`

Peringatan dan rekomendasi kinerja

FSx untuk ONTAP menampilkan peringatan untuk CloudWatch metrik setiap kali salah satu metrik ini mendekati atau melewati ambang batas yang telah ditentukan untuk beberapa titik data berturut-turut. Peringatan ini memberi Anda rekomendasi yang dapat ditindaklanjuti yang dapat Anda gunakan untuk mengoptimalkan kinerja sistem file Anda.

Peringatan dapat diakses di beberapa area dasbor Pemantauan & kinerja. Semua peringatan kinerja Amazon FSx aktif atau terbaru dan CloudWatch alarm apa pun yang dikonfigurasi untuk sistem file yang berada dalam status ALARM muncul di panel Pemantauan & kinerja di bagian Ringkasan. Peringatan juga muncul di bagian dasbor tempat grafik metrik ditampilkan.

Anda dapat membuat CloudWatch alarm untuk salah satu metrik Amazon FSx. Untuk informasi selengkapnya, lihat Membuat CloudWatch alarm Amazon untuk memantau Amazon FSx.

Gunakan peringatan kinerja untuk meningkatkan kinerja sistem file

Amazon FSx memberikan rekomendasi yang dapat ditindaklanjuti yang dapat Anda gunakan untuk mengoptimalkan kinerja sistem file Anda. Rekomendasi ini menjelaskan bagaimana Anda dapat mengatasi leher botol kinerja potensial. Anda dapat mengambil tindakan yang disarankan jika Anda mengharapkan aktivitas berlanjut, atau jika itu menyebabkan dampak pada kinerja sistem file Anda. Bergantung pada metrik mana yang memicu peringatan, Anda dapat menyelesaikannya dengan meningkatkan kapasitas throughput atau kapasitas penyimpanan sistem file, seperti yang dijelaskan dalam tabel berikut.

Bagian dasbor	Jika ada peringatan untuk metrik ini	Lakukan hal berikut
Penyimpanan	Pemanfaatan kapasitas penyimpanan primer	Tingkatkan kapasitas penyimpanan utama sistem file Anda jika sistem file Anda belum mencapai kapasitas penyimpanan SSD maksimum. Untuk informasi selengkapnya, lihat Memodifikasi kapasitas penyimpanan SSD dan IOPS yang disediakan. Jika sistem file Anda memiliki beberapa pasangan HA dan pemanfaatan kapasitas penyimpanan utama Anda hanya lebih tinggi untuk subset agregat sistem file Anda (kumpulan penyimpanan yang membentuk tingkat penyimpanan utama Anda), maka Anda juga dapat menyeimbangkan kembali beban kerja Anda sehingga pemanfaatan kapasitas penyimpanan utama Anda lebih merata di seluruh sistem file Anda. Untuk informasi selengkapnya tentang menyeimbangkan kembali beban kerja Anda, lihat. Memantau FSx untuk keseimbangan beban kerja ONTAP

Bagian dasbor	Jika ada peringatan untuk metrik ini	Lakukan hal berikut
Kinerja server file	Throughput jaringan Throughput disk IOPS Disk Pemanfaatan CPU	Tingkatkan kapasitas throughput sistem file Anda jika sistem file Anda belum mencapai kapasitas throughput maksimum. Untuk informasi selengkapnya tentang memperbarui kapasitas throughput, lihatBagaimana cara mengubah kapasitas throughput. Jika sistem file Anda memiliki beberapa pasangan HA dan pemanfaatannya tinggi hanya untuk sebagian dari server file, maka Anda juga dapat menyeimbangkan kembali beban kerja Anda sehingga beban kerja Anda lebih merata memanfaatkan kemampuan kinerja masing-masing pasangan HA sistem file Anda. Untuk informasi selengkapnya tentang menyeimbangkan kembali beban kerja Anda, lihat. Memantau FSx untuk keseimbangan beban kerja ONTAP
Performa disk	IOPS Disk	Tingkatkan IOPS SSD jika sistem file Anda belum mencapai IOPS SSD maksimum untuk kapasitas throughput sistem file Anda saat ini. Untuk informasi selengkapnya tentang memperbarui IOPS yang disediakan sistem file Anda, lihat. Memodifikasi kapasitas penyimpanan SSD dan IOPS yang disediakan Jika sistem file Anda memiliki beberapa pasangan HA dan pemanfaatan IOPS disk Anda hanya lebih tinggi untuk subset agregat sistem file Anda (kumpulan penyimpanan yang membentuk tingkat penyimpanan utama Anda), maka Anda juga dapat menyeimbangkan kembali beban kerja Anda sehingga IOPS disk Anda digunakan lebih merata di seluruh sistem file Anda. Untuk informasi selengkapnya tentang menyeimbangkan kembali beban kerja Anda, lihat. Memantau FSx untuk keseimbangan beban kerja ONTAP

Untuk informasi selengkapnya tentang kinerja sistem file, lihatAmazon FSx untuk NetApp kinerja ONTAP.

Membuat CloudWatch alarm Amazon untuk memantau Amazon FSx

Anda dapat membuat CloudWatch alarm yang mengirimkan pesan Amazon Simple Notification Service (Amazon SNS) saat alarm berubah status. Alarm mengawasi metrik tunggal selama periode waktu yang Anda tentukan. Jika diperlukan, alarm kemudian melakukan satu atau lebih tindakan berdasarkan nilai metrik relatif terhadap ambang batas tertentu selama beberapa periode waktu. Tindakan ini adalah notifikasi yang dikirim ke topik Amazon SNS atau kebijakan Penskalaan Otomatis.

Alarm memanggil tindakan untuk perubahan status berkelanjutan saja. CloudWatch alarm tidak memanggil tindakan hanya karena mereka berada dalam keadaan tertentu; negara harus telah berubah dan dipertahankan untuk sejumlah periode tertentu. Anda dapat membuat alarm dari konsol Amazon FSx atau konsol Amazon CloudWatch .

Prosedur berikut menjelaskan cara membuat alarm menggunakan konsol Amazon FSx AWS Command Line Interface ,AWS CLI(), dan API.

Untuk mengatur alarm menggunakan konsol Amazon FSx

1. Buka konsol Amazon FSx di https://console.aws.amazon.com/fsx/.
2. Di panel navigasi kiri, pilih Sistem file, lalu pilih sistem file yang ingin Anda buat alarm.
3. Pada halaman Ringkasan, pilih Pemantauan & kinerja dari panel kedua.
4. Pilih tab CloudWatch alarm.
5. Pilih Buat CloudWatch alarm. Anda dialihkan ke konsol CloudWatch.
6. Pilih Pilih Metrik.
7. Di bagian Metrik, pilih FSx.
8. Pilih kategori metrik:
   - Metrik Sistem File
   - Metrik Sistem File Terperinci
   - Metrik Volume
   - Metrik Volume Terperinci
9. Pilih metrik yang ingin Anda atur alarmnya, lalu pilih Pilih metrik.

10. Di bagian Kondisi, pilih kondisi yang Anda inginkan untuk alarm, lalu pilih Berikutnya.

> **Note**
>
> Metrik mungkin tidak dipublikasikan selama pemeliharaan sistem file. Untuk mencegah perubahan kondisi alarm yang tidak perlu dan menyesatkan dan mengonfigurasi alarm Anda agar tahan terhadap titik data yang hilang, lihat Mengonfigurasi cara CloudWatch alarm menangani data yang hilang di Panduan Pengguna Amazon. CloudWatch

11. Jika Anda CloudWatch ingin mengirimi Anda email atau pemberitahuan Amazon SNS saat status alarm memulai tindakan, pilih status alarm untuk Pemicu status alarm.

    Untuk Kirim pemberitahuan ke topik SNS berikut, pilih opsi. Jika memilih Buat topik, Anda dapat mengatur nama dan alamat email untuk daftar langganan email baru. Daftar ini disimpan dan muncul dalam bidang isian untuk alarm selanjutnya. Pilih Selanjutnya.

> **Note**
>
> Jika Anda menggunakan Buat topik untuk membuat topik Amazon SNS yang baru, alamat email harus diverifikasi sebelum menerima pemberitahuan. Email hanya dikirim saat alarm memasuki status alarm. Jika perubahan keadaan alarm ini terjadi sebelum alamat email diverifikasi, alamat tidak akan menerima pemberitahuan.

12. Isi kolom Nama alarm dan deskripsi Alarm, lalu pilih Berikutnya.
13. Pada halaman Pratinjau dan buat, tinjau alarm yang akan Anda buat, lalu pilih Buat alarm.

Untuk mengatur alarm menggunakan konsol CloudWatch

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pilih Buat Alarm Untuk memulai Wizard Buat Alarm.
3. Ikuti prosedur di Untuk mengatur alarm menggunakan konsol Amazon FSx, dimulai dengan langkah 6.

Untuk mengatur alarm menggunakan AWS CLI

- Panggil perintah CLI put-metric-alarm. Untuk informasi selengkapnya, lihat Referensi Perintah AWS AWS CLI.

Untuk mengatur alarm menggunakan CloudWatch API

- Panggil operasi PutMetricAlarm API. Untuk informasi selengkapnya, lihat Referensi Amazon CloudWatch API.

Memantau FSx untuk keseimbangan beban kerja ONTAP

Jika Anda memiliki sistem file dengan beberapa pasangan HA, maka kinerja dan throughputnya tersebar di setiap pasangan HA Anda. FSx untuk ONTAP secara otomatis menyeimbangkan file Anda saat ditulis ke sistem file Anda, tetapi dalam kasus yang jarang terjadi, data beban kerja atau I/O Anda dapat menjadi tidak seimbang di seluruh pasangan HA, yang dapat memengaruhi kinerja keseluruhan beban kerja Anda. Anda dapat memantau beban kerja Anda untuk memastikan bahwa itu tetap seimbang di setiap pasangan HA sistem file Anda (dan server file dan agregat yang sepadan - kumpulan penyimpanan yang membentuk tingkat penyimpanan utama Anda).

Topik

Saldo pemanfaatan penyimpanan primer

Kapasitas penyimpanan utama sistem file Anda dibagi secara merata di antara masing-masing pasangan HA Anda di kumpulan penyimpanan yang disebut agregat. Setiap pasangan HA memiliki satu agregat. Kami menyarankan Anda mempertahankan pemanfaatan rata-rata tidak lebih dari 80% untuk tingkat penyimpanan utama Anda secara berkelanjutan. Untuk sistem file dengan beberapa pasangan HA, kami menyarankan Anda mempertahankan pemanfaatan rata-rata hingga 80% untuk setiap agregat.

Mempertahankan pemanfaatan 80% memastikan ada ruang kosong untuk data baru yang masuk, dan mempertahankan overhead yang sehat untuk operasi pemeliharaan yang sementara dapat mengklaim ruang kosong pada agregat Anda.

Jika Anda melihat bahwa agregat Anda tidak seimbang, Anda dapat meningkatkan kapasitas penyimpanan utama sistem file Anda (sepadan dengan meningkatkan kapasitas penyimpanan

setiap agregat), atau Anda dapat memindahkan volume Anda antar agregat menggunakan perintah pemindahan volume di CLI ONTAP.

Ketidakseimbangan pemanfaatan kinerja file server dan disk

Kemampuan kinerja total sistem file Anda (seperti throughput jaringan, file server ke throughput disk dan IOPS, dan IOPS disk) dibagi secara merata di antara pasangan HA sistem file Anda. Kami menyarankan Anda mempertahankan pemanfaatan rata-rata di bawah 50% (dan pemanfaatan puncak maksimum di bawah 80%) untuk semua batas kinerja secara berkelanjutan—ini berlaku untuk pemanfaatan keseluruhan sumber daya server file sistem file Anda di semua pasangan HA, serta pada basis server per file.

Jika Anda melihat bahwa pemanfaatan kinerja server file Anda tidak seimbang—dan server file di mana beban kerja Anda tidak seimbang memiliki pemanfaatan berkelanjutan lebih dari 80% —Anda dapat menggunakan ONTAP CLI dan REST API untuk mendiagnosis lebih lanjut penyebab ketidakseimbangan kinerja dan memperbaikinya. Berikut ini adalah tabel indikator ketidakseimbangan yang mungkin dan langkah selanjutnya untuk diagnosis lebih lanjut.

Jika sistem file Anda...	Maka...
Throughput disk server file atau IOPS disk server file tidak seimbang	Anda mungkin mengalami hotspotting I/O pada subset pasangan HA (subset volume Anda yang berisi sejumlah besar data yang diakses) yang dapat membatasi kinerja keseluruhan beban kerja Anda karena terhambat terhadap subset pasangan HA. Untuk setiap server file yang sangat digunakan, periksa volume yang paling banyak digunakan untuk melihat volume mana yang memiliki aktivitas paling banyak dalam agregat. Untuk informasi lebih lanjut tentang prosedur ini, lihatMenyeimbangkan kembali volume yang sangat dimanfaatkan.
Throughput jaringan tidak seimbang, tetapi throughput disk server file Anda, IOPS disk server file, atau IOPS disk Anda tidak seimbang	Data Anda didistribusikan secara merata di seluruh pasangan HA, tetapi klien Anda tidak. Untuk server file yang memiliki lebih banyak pemanfaat an throughput jaringan daripada yang lain, periksa klien teratas untuk setiap server file, kemudian menyeimbangkan kembali klien tersebut dengan melepas volume apa pun dari klien tersebut dan mengatur ulang mereka menggunakan titik akhir yang berbeda pada pasangan HA yang berbeda. Untuk informasi lebih lanjut tentang prosedur ini, lihatMenyeimbangkan kembali klien dengan lalu lintas tinggi.

Memetakan CloudWatch dimensi ke sumber daya ONTAP CLI dan REST API

Sistem file scale-out Anda memiliki CloudWatch metrik Amazon dengan dimensi atau. `FileServer` `Aggregate` Untuk mendiagnosis lebih lanjut kasus ketidakseimbangan, Anda perlu memetakan nilai dimensi ini ke server file tertentu (atau node) dan agregat di ONTAP CLI atau REST API.

- Untuk server file, setiap nama server file memetakan ke nama server file (atau node) di ONTAP (misalnya,`FsxId01234567890abcdef-01`). Server file bernomor ganjil adalah server file yang disukai (yaitu, mereka melayani lalu lintas kecuali sistem file gagal ke server file sekunder), sedangkan server file bernomor genap adalah server file sekunder (yaitu, mereka melayani lalu lintas hanya ketika mitra mereka tidak tersedia). Karena itu, server file sekunder biasanya akan menunjukkan pemanfaatan yang lebih sedikit daripada server file pilihan.
- Untuk agregat, setiap nama agregat memetakan ke agregat di ONTAP (misalnya,). `aggr1` Ada satu agregat untuk setiap pasangan HA, artinya agregat `aggr1` dibagikan oleh server file `FsxId01234567890abcdef-01` (server file aktif) dan `FsxId01234567890abcdef-02` (server file sekunder) dalam pasangan HA, agregat `aggr2` dibagikan oleh server file `FsxId01234567890abcdef-03` dan`FsxId01234567890abcdef-04`, dan seterusnya.

Anda dapat melihat pemetaan antara semua agregat dan server file menggunakan CLI ONTAP.

1. Untuk SSH ke NetApp CLI ONTAP sistem file Anda, ikuti langkah-langkah yang didokumentasikan di bagian Panduan Pengguna Amazon FSx untuk ONTAP. Menggunakan CLI NetApp ONTAP NetApp

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Gunakan perintah show agregat penyimpanan, tentukan parameternya`-fields node`.

   ```
   ::> storage aggregate show -fields node
   aggregate                     node
   ----------------------------- -------------------------
   aggr1                         FsxId01234567890abcdef-01
   aggr2                         FsxId01234567890abcdef-03
   aggr3                         FsxId01234567890abcdef-05
   aggr4                         FsxId01234567890abcdef-07
   aggr5                         FsxId01234567890abcdef-09
   aggr6                         FsxId01234567890abcdef-11
   ```

```
6 entries were displayed.
```

Menyeimbangkan kembali klien dengan lalu lintas tinggi

Jika Anda mengalami ketidakseimbangan I/O di seluruh server file (khususnya dengan pemanfaatan throughput Jaringan), klien I/O yang tinggi mungkin menjadi penyebabnya. Untuk mengidentifikasi klien dengan lalu lintas tinggi, gunakan CLI ONTAP.

1. Untuk SSH ke NetApp CLI ONTAP sistem file Anda, ikuti langkah-langkah yang didokumentasikan di bagian Panduan Pengguna Amazon FSx untuk ONTAP. Menggunakan CLI NetApp ONTAP NetApp

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Untuk melihat klien dengan lalu lintas tertinggi, gunakan statistik klien teratas yang menunjukkan perintah CLI ONTAP. Anda dapat secara opsional menentukan `-node` parameter untuk hanya melihat klien teratas untuk server file tertentu. Jika Anda mendiagnosis ketidakseimbangan untuk server file tertentu, gunakan `-node` parameter, ganti `node_name` dengan nama server file (misalnya,`FsxId01234567890abcdef-01`).

   Anda dapat menambahkan `-interval` parameter secara opsional, memberikan interval untuk mengukur (dalam detik) sebelum setiap laporan dikeluarkan. Meningkatkan interval (misalnya, hingga maksimum 300 detik) memberikan sampel jangka panjang untuk jumlah lalu lintas yang didorong ke setiap volume. Defaultnya adalah 5 (detik).

   ```
   ::> statistics top client show -node FsxId01234567890abcdef-01 [-interval [5,300]]
   ```

   Dalam output, klien teratas ditunjukkan oleh alamat IP dan port mereka.

   ```
                                                  *Total     Total
              Client   Vserver          Node          Ops     (Bps)
   ------------------ --------- ------------------------ ------ ---------
    172.17.236.53:938 svm01     FsxId01234567890abcdef-01   2143 140443648
   172.17.236.160:898 svm02     FsxId01234567890abcdef-01    812  53215232
   ```

3. Anda dapat menyeimbangkan kembali subset klien lalu lintas tinggi yang terdaftar ke server file lain. Untuk melakukannya, lepaskan volume dari klien dan pasang kembali menggunakan nama

DNS untuk titik akhir NFS/SMB SVM—ini mengembalikan titik akhir acak yang sesuai dengan pasangan HA acak.

Kami menyarankan Anda menggunakan kembali nama DNS, tetapi Anda memiliki opsi untuk secara eksplisit memilih pasangan HA mana yang dipasang klien tertentu. Untuk menjamin bahwa Anda memasang klien ke titik akhir yang berbeda, Anda dapat menentukan alamat IP titik akhir yang berbeda dari yang sesuai dengan node yang mengalami lalu lintas tinggi. Anda dapat melakukannya dengan menjalankan perintah berikut:

```
::> network interface show -vserver svm_name -lif nfs_smb_management* -fields
 address,curr-node
vserver   lif                  address      curr-node
--------- -------------------- ------------ ------------------------
svm01 nfs_smb_management_1 172.31.15.89 FsxId01234567890abcdef-01
svm01 nfs_smb_management_3 172.31.8.112 FsxId01234567890abcdef-03
2 entries were displayed.
```

Menurut contoh output untuk `statistics top client show` perintah, klien `172.17.236.53` mengarahkan lalu lintas tinggi ke`FsxId01234567890abcdef-01`. Output dari `network interface show` perintah menunjukkan ini adalah alamatnya`172.31.15.89`. Untuk me-mount ke titik akhir yang berbeda, pilih alamat lain (dalam contoh ini, satu-satunya alamat lainnya adalah`172.31.8.112`, sesuai dengan`FsxId01234567890abcdef-03`).

Menyeimbangkan kembali volume yang sangat dimanfaatkan

Jika Anda mengalami ketidakseimbangan I/O di seluruh volume atau agregat, Anda dapat menyeimbangkan kembali volume untuk mendistribusikan kembali lalu lintas I/O di seluruh volume Anda.

> **Note**
>
> Jika Anda mengalami ketidakseimbangan pemanfaatan penyimpanan di seluruh agregat Anda, umumnya tidak ada dampak kinerja kecuali pemanfaatan yang tinggi digabungkan dengan ketidakseimbangan I/O. Meskipun Anda dapat memindahkan volume antar agregat untuk menyeimbangkan pemanfaatan penyimpanan, kami sarankan hanya memindahkan volume jika Anda melihat dampak kinerja, karena volume bergerak dapat berdampak buruk

pada kinerja jika Anda juga tidak mempertimbangkan I/O yang didorong ke setiap volume yang Anda pertimbangkan untuk dipindahkan.

1. Untuk SSH ke NetApp CLI ONTAP sistem file Anda, ikuti langkah-langkah yang didokumentasikan di bagian Panduan Pengguna Amazon FSx untuk ONTAP. Menggunakan CLI NetApp ONTAP NetApp

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Gunakan perintah statistik volume show ONTAP CLI untuk melihat volume lalu lintas tertinggi untuk agregat tertentu, dengan perubahan berikut:

   - Ganti *aggregate_name dengan nama* agregat (misalnya,). `aggr1`
   - Anda dapat menambahkan `-interval` parameter secara opsional, memberikan interval untuk mengukur (dalam detik) sebelum setiap laporan dikeluarkan. Meningkatkan interval (misalnya, hingga maksimum 300 detik) memberikan sampel jangka panjang untuk jumlah lalu lintas yang didorong ke setiap volume. Defaultnya adalah 5 (detik).

```
::> statistics volume show -aggregate aggregate_name -sort-key total_ops [-interval
 [5,300]]
```

Tergantung pada interval yang Anda pilih, dibutuhkan waktu hingga 5 menit untuk menampilkan data. Perintah menunjukkan semua volume dalam agregat, bersama dengan jumlah lalu lintas yang didorong ke setiap agregat.

```
                          *Total Read Write Other      Read Write Latency
    Volume Vserver Aggregate    Ops  Ops   Ops   Ops     (Bps) (Bps)    (us)
---------- ------- --------- ------ ---- ----- ----- --------- ----- -------
vol1__0007    svm1     aggr1   4078 4078     0     0 267255808     0    1092
vol1__0005    svm1     aggr1   4078 4078     0     0 267255808     0    1086
vol1__0003    svm1     aggr1   4077 4077     0     0 267223040     0    1086
vol1__0001    svm1     aggr1   4077 4077     0     0 267239424     0    1087
vol1__0008    svm1     aggr2   2314 2314     0     0 151650304     0    1112
vol1__0006    svm1     aggr2   2144 2144     0     0 140509184     0    1104
vol1__0002    svm1     aggr2   2183 2183     0     0 143065088     0    1106
vol1__0004    svm1     aggr2   2183 2183     0     0 143065088     0    1103
```

Statistik volume ditampilkan berdasarkan per-konstituen (misalnya, `vol1__0015` adalah konstituen ke-15 untuk). FlexGroup `vol1` Anda dapat melihat dari contoh output, konstituen untuk lebih banyak `aggr1` digunakan daripada konstituen untuk. `aggr2` Untuk menyeimbangkan lalu lintas antar agregat, Anda dapat memindahkan volume konstituen antar agregat sehingga lalu lintas lebih merata.

3. Untuk memindahkan volume antar agregat, gunakan perintah volume move start ONTAP CLI, ganti nilai berikut:

   - Ganti *`svm_name`* dengan nama SVM yang menampung volume yang Anda pindahkan.
   - Ganti *`volume_name`* dengan nama konstituen volume (misalnya,). `vol1__0001`
   - Ganti *`aggregate_name`* dengan nama agregat tujuan untuk volume.

   > **Important**
   >
   > Gerakan volume mengkonsumsi sumber daya jaringan dan disk untuk server file sumber dan tujuan. Akibatnya, kinerja beban kerja Anda dapat dipengaruhi oleh pergerakan volume yang sedang berlangsung. Selain itu, ada fase cut-over dari proses pergerakan volume yang sementara menjeda I/O untuk setiap lalu lintas ke volume.

```
::> volume move start -vserver svm_name -volume volume_name -
destination aggregate_name -foreground false
[Job 1] Job is queued: Move "vol1__0001" in Vserver "svm01" to aggregate "aggr1".
Use the "volume move show -vserver svm01 -volume vol1__0001" command to view the
 status of this operation.
```

Untuk memeriksa status operasi pemindahan volume, gunakan perintah `volume move show` ONTAP CLI.

```
::> volume move show -vserver svm_name -volume volume_name
                            Vserver Name: svm01
                             Volume Name: vol1__0001
                    Actual Completion Time: -
                           Bytes Remaining: 1.00TB
              Specified Action For Cutover: retry_on_failure
            Specified Cutover Time Window: 30
                   Destination Aggregate: aggr2
```

```
                    Destination Node: FsxId01234567890abcdef-03
                     Detailed Status: Transferring data: 12.23GB sent.
                  Percentage Complete: 1%
                           Move Phase: replicating
      Prior Issues Encountered: -
Estimated Remaining Duration: 00:40:25
        Replication Throughput: 434.3MB/s
              Duration of Move: 00:00:27
              Source Aggregate: aggr2
                   Source Node: FsxId01234567890abcdef-01
                    Move State: healthy
```

Perintah ini menunjukkan perkiraan waktu untuk menyelesaikan langkah, sebagai salah satu bidang informasi. Ketika operasi selesai, perintah yang sama akan menunjukkan bahwa `Move Phase` bidang selesai.

Anda harus memastikan bahwa masing-masing didistribusikan FlexGroup secara merata di seluruh agregat Anda, idealnya dengan 8 konstituen yang direkomendasikan per agregat. Jika Anda memindahkan satu volume konstituen ke agregat lain untuk seimbangFlexGroup, Anda pada gilirannya harus memindahkan volume konstituen lain (yang kurang digunakan) ke agregat sumber untuk menjaga keseimbangan.

Memantau fsX untuk acara ONTAP EMS

Anda dapat memantau FSx untuk peristiwa sistem file ONTAP menggunakan Sistem Manajemen Acara (EMS) asli NetApp ONTAP. Anda dapat melihat peristiwa ini menggunakan CLI NetApp ONTAP.

Topik

- Ikhtisar acara EMS
- Melihat acara EMS
- Penerusan acara EMS ke server Syslog

Ikhtisar acara EMS

Acara EMS secara otomatis menghasilkan pemberitahuan yang mengingatkan Anda ketika kondisi yang telah ditentukan terjadi di fsX Anda untuk sistem file ONTAP. Pemberitahuan ini memberi Anda

informasi sehingga Anda dapat mencegah atau memperbaiki masalah yang dapat menyebabkan masalah yang lebih besar, seperti masalah otentikasi mesin virtual penyimpanan (SVM) atau volume penuh.

Secara default, peristiwa dicatat dalam log Sistem Manajemen Acara. Dengan menggunakan EMS, Anda dapat memantau peristiwa seperti perubahan kata sandi pengguna, konstituen dalam kapasitas penuh yang FlexGroup mendekati, Nomor Unit Logika (LUN) secara manual dibawa online atau offline, atau mengubah ukuran volume secara otomatis.

Untuk informasi selengkapnya tentang peristiwa ONTAP EMS, lihat Referensi ONTAP EMS di Pusat Dokumentasi NetApp ONTAP. Untuk menampilkan kategori acara, gunakan panel navigasi kiri dokumen.

> **Note**
>
> Hanya beberapa pesan EMS ONTAP yang tersedia untuk fsX untuk sistem file ONTAP. Untuk melihat daftar pesan EMS ONTAP yang tersedia, gunakan perintah pertunjukan katalog acara NetApp CLI ONTAP.

Deskripsi acara EMS berisi nama peristiwa, tingkat keparahan, kemungkinan penyebab, pesan log, dan tindakan korektif yang dapat membantu Anda memutuskan cara merespons. Misalnya, peristiwa Wafl.vol.autosize.fail terjadi ketika ukuran otomatis volume gagal. Menurut deskripsi acara, tindakan korektif adalah meningkatkan ukuran maksimum volume saat mengatur ukuran otomatis.

Melihat acara EMS

Gunakan perintah NetApp ONTAP CLI event log show untuk menampilkan isi log peristiwa. Perintah ini tersedia jika Anda memiliki `fsxadmin` peran pada sistem file Anda. Sintaks perintah adalah sebagai berikut:

```
event log show [event_options]
```

Peristiwa terbaru terdaftar terlebih dahulu. Secara default, perintah ini menampilkan`EMERGENCY`,`ALERT`, dan peristiwa `ERROR` tingkat keparahan dengan informasi berikut:

- Waktu - Waktu acara.
- Node — Node di mana peristiwa itu terjadi.

- Keparahan — Tingkat keparahan acara. Untuk menampilkan`NOTICE`,`INFORMATIONAL`, atau peristiwa `DEBUG` tingkat keparahan, gunakan opsi. `-severity`
- Event — Nama dan pesan acara.

Untuk menampilkan informasi rinci tentang peristiwa, gunakan satu atau beberapa opsi acara yang tercantum dalam tabel berikut.

Opsi acara	Deskripsi
`-detail`	Menampilkan informasi acara tambahan.
`-detailtime`	Menampilkan informasi acara terperinci dalam urutan kronologis terbalik.
`-instance`	Menampilkan informasi rinci tentang semua bidang.
`-node` *`nodename`*`|local`	Menampilkan daftar peristiwa untuk node yang Anda tentukan. Gunakan opsi ini `-seqnum` untuk menampilkan informasi terperinci.
`-seqnum` *`sequence_number`*	Memilih peristiwa yang cocok dengan nomor ini dalam urutan. Gunakan dengan `-node` untuk menampilkan informasi rinci.
`-time` *`MM/DD/YYYY HH:MM:SS`*	Memilih peristiwa yang terjadi pada waktu tertentu ini. Gunakan format: MM/DD/YYYY HH: MM: SS [+- HH: MM]. Anda dapat menentukan rentang waktu dengan

Opsi acara	Deskripsi

	menggunakan `..` operator antara dua pernyataan waktu.
	
	`event log show -time "04/17/2023 05:55:00".."04/17/2023 06:10:00"`
	
	Nilai waktu komparatif relatif terhadap waktu saat ini ketika Anda menjalankan perintah. Contoh berikut menunjukkan cara menampilkan hanya peristiwa yang terjadi dalam menit terakhir:
	
	`event log show -time >1m`
	
	Bidang bulan dan tanggal opsi ini tidak empuk nol. Bidang ini dapat berupa digit tunggal; misalnya,`4/1/2023 06:45:00`.

Opsi acara	Deskripsi
`-severity sev_level`	Memilih peristiwa yang cocok dengan nilai *sev_level* , yang harus menjadi salah satu dari berikut ini: • `EMERGENCY` — Gangguan • `ALERT`— Titik kegagalan tunggal • `ERROR`- Degradasi • `NOTICE`— Informasi • `INFORMATIONAL` — Informasi • `DEBUG`— Informasi debug Untuk menampilkan semua acara, tentukan tingkat keparahan sebagai berikut: `event log show -severity <=DEBUG`

Opsi acara	Deskripsi
`-ems-severity` *ems_sev_level*	Memilih peristiwa yang cocok dengan nilai *ems_sev_level*, yang harus menjadi salah satu dari berikut ini: • `NODE_FAULT` Korupsi data terdeteksi atau node tidak dapat menyediakan layanan klien. • `SVC_FAULT` — Kehilangan layanan sementara — biasanya kesalahan perangkat lunak sementara — terdeteksi. • `NODE_ERROR` — Kesalahan perangkat keras yang tidak langsung fatal terdeteksi. • `SVC_ERROR` — Kesalahan perangkat lunak yang tidak langsung fatal terdeteksi. • `WARNING`— Pesan prioritas tinggi yang tidak menunjukkan kesalahan. • `NOTICE`— Pesan prioritas normal yang tidak menunjukkan kesalahan. • `INFO`— Pesan prioritas rendah yang tidak menunjukkan kesalahan. • `DEBUG`— Pesan debugging. • `VAR`— Pesan dengan tingkat keparahan variabel, dipilih saat runtime.

Opsi acara	Deskripsi
	Untuk menampilkan semua acara, tentukan tingkat keparahan sebagai berikut: `event log show -ems-severity <=DEBUG`
`-source` *`text`*	Memilih peristiwa yang cocok dengan nilai *`teks`*. Sumbernya biasanya modul perangkat lunak.
`-message-name` *`message_name`*	Memilih peristiwa yang cocok dengan nilai *`message_name`* . Nama pesan bersifat deskriptif, sehingga menyaring output dengan nama pesan menampilkan pesan dari jenis tertentu.
`-event` *`text`*	Memilih peristiwa yang cocok dengan nilai *`teks`*. `event`Bidang berisi teks lengkap acara, termasuk parameter apa pun.
`-kernel-generation-num` *`integer`*	Memilih peristiwa yang cocok dengan *`nilai integer`*. Hanya peristiwa yang berasal dari kernel yang memiliki nomor pembuatan kernel.

Opsi acara	Deskripsi
`-kernel-sequence-num` *integer*	Memilih peristiwa yang cocok dengan *nilai integer*. Hanya peristiwa yang berasal dari kernel yang memiliki nomor urut kernel.
`-action` *text*	Memilih peristiwa yang cocok dengan nilai *teks*. `action`Bidang ini menjelaskan tindakan korektif apa, jika ada, yang harus Anda ambil untuk memperbaiki situasi.
`-description` *text*	Memilih peristiwa yang cocok dengan nilai *teks*. `description` Bidang ini menjelaskan mengapa peristiwa itu terjadi dan apa artinya.
`-filter-name` *filter_name*	Memilih peristiwa yang cocok dengan nilai *filter_name* . Hanya peristiwa yang disertakan oleh filter yang ada yang cocok dengan tampilan nilai ini.
`-fields` *fieldname* `,...`	Menunjukkan bahwa output perintah juga mencakup bidang atau bidang yang ditentukan. Anda dapat menggunakan `-fields ?` untuk memilih bidang yang ingin Anda tentukan.

Untuk melihat acara EMS

1. Untuk SSH ke NetApp CLI ONTAP sistem file Anda, ikuti langkah-langkah yang didokumentasikan di bagian Panduan Pengguna Amazon FSx untuk ONTAP. Menggunakan CLI NetApp ONTAP NetApp

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Gunakan `event log show` perintah untuk menampilkan isi log peristiwa.

   ```
   ::> event log show
   Time                Node          Severity      Event
   ------------------- ------------- ------------- ------------------------
   6/30/2023 13:54:19  node1         NOTICE        vifmgr.portup: A link up event was
    received on node node1, port e0a.
   6/30/2023 13:54:19  node1         NOTICE        vifmgr.portup: A link up event was
    received on node node1, port e0d.
   ```

Untuk informasi tentang peristiwa EMS yang dikembalikan oleh `event log show` perintah, lihat Referensi EMS ONTAP di Pusat Dokumentasi NetApp ONTAP.

Penerusan acara EMS ke server Syslog

Anda dapat mengonfigurasi acara EMS untuk meneruskan pemberitahuan ke server Syslog. Penerusan acara EMS digunakan untuk pemantauan real-time sistem file Anda untuk menentukan dan mengisolasi akar penyebab untuk berbagai masalah. Jika lingkungan Anda belum berisi server Syslog untuk pemberitahuan acara, Anda harus membuatnya terlebih dahulu. DNS harus dikonfigurasi pada sistem file untuk menyelesaikan nama server Syslog.

Untuk mengonfigurasi peristiwa EMS untuk meneruskan pemberitahuan ke server Syslog

1. Untuk SSH ke NetApp CLI ONTAP sistem file Anda, ikuti langkah-langkah yang didokumentasikan di bagian Panduan Pengguna Amazon FSx untuk ONTAP. Menggunakan CLI NetApp ONTAP NetApp

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Gunakan perintah buat tujuan pemberitahuan acara untuk membuat tujuan pemberitahuan acara dari jenis`syslog`, menentukan atribut berikut:

- *dest_name*— Nama tujuan notifikasi yang akan dibuat (misalnya,`syslog-ems`). Nama tujuan pemberitahuan acara harus memiliki panjang 2 hingga 64 karakter. Karakter yang valid adalah karakter ASCII berikut: A-Z, a-z, 0-9, "_", dan "-". Nama harus dimulai dan diakhiri dengan: A-Z, a-z, atau 0-9.
- *syslog_name*— Nama host server Syslog atau alamat IP yang mengirim pesan Syslog.
- *transport_protocol*— Protokol yang digunakan untuk mengirim acara:
  - `udp-unencrypted`— Protokol Datagram Pengguna tanpa keamanan. Ini adalah protokol default.
  - `tcp-unencrypted`— Protokol Kontrol Transmisi tanpa keamanan.
  - `tcp-encrypted`— Protokol Kontrol Transmisi dengan Transport Layer Security (TLS). Ketika opsi ini ditentukan, FSx untuk ONTAP memverifikasi identitas host tujuan dengan memvalidasi sertifikatnya.
- *port_number*— Port server Syslog tempat pesan Syslog dikirim ke. `syslog-port`Parameter nilai default tergantung pada pengaturan untuk `syslog-transport` parameter. Jika `syslog-transport` diatur ke`tcp-encrypted`, nilai `syslog-port` defaultnya adalah`6514`. Jika `syslog-transport` diatur ke`tcp-unencrypted`, `syslog-port` memiliki nilai default`601`. Jika tidak, port default diatur ke`514`.

```
::> event notification destination create -name dest_name -syslog syslog_name -
syslog-transport transport_protocol -syslog-port port_number
```

3. Gunakan perintah buat pemberitahuan acara untuk membuat pemberitahuan baru dari serangkaian peristiwa yang ditentukan oleh filter peristiwa ke tujuan notifikasi yang dibuat pada langkah sebelumnya, dengan menentukan atribut berikut:

   - *node_name*— Nama filter acara. Peristiwa yang termasuk dalam filter acara diteruskan ke tujuan yang ditentukan dalam parameter. `-destinations`
   - *dest_name*— Nama tujuan notifikasi yang ada tempat pemberitahuan acara dikirim.

```
::> event notification create -filter-name filter_name -destinations dest_name
```

4. Gunakan `event notification destination check` perintah untuk menghasilkan pesan pengujian dan verifikasi penyiapan Anda berfungsi. Tentukan atribut berikut dengan perintah:

   - *node_name*— Nama simpul (misalnya,`FsxId07353f551e6b557b4-01`).

- *dest_name*— Nama tujuan notifikasi yang ada tempat pemberitahuan acara dikirim.

```
::> set diag
::*> event notification destination check -node node_name -destination-
name dest_name
```

Pemantauan dengan Cloud Insights

NetApp Cloud Insights adalah NetApp layanan yang dapat Anda gunakan untuk memantau Amazon fsX Anda NetApp untuk sistem file ONTAP bersama solusi penyimpanan Anda NetApp yang lain. Dengan Cloud Insights, Anda dapat memantau metrik konfigurasi, kapasitas, dan kinerja dari waktu ke waktu untuk memahami tren beban kerja Anda dan merencanakan kinerja masa depan dan kebutuhan kapasitas penyimpanan. Anda juga dapat membuat peringatan berdasarkan kondisi metrik yang dapat diintegrasikan dengan alur kerja dan alat produktivitas yang ada.

> **Note**
>
> Cloud Insights tidak didukung untuk sistem file scale-out.

Cloud Insights menyediakan:

- Luasnya metrik dan log — Kumpulkan metrik konfigurasi, kapasitas, dan kinerja. Pahami bagaimana beban kerja Anda menjadi tren dengan dasbor, peringatan, dan laporan yang telah ditentukan sebelumnya.
- Analitik pengguna dan perlindungan ransomware — Dengan snapshot Cloud Secure dan ONTAP Anda dapat mengaudit, mendeteksi, menghentikan, dan memperbaiki insiden kesalahan pengguna dan ransomware.
- SnapMirror pelaporan — Pahami SnapMirror hubungan Anda dan tetapkan peringatan tentang masalah replikasi.
- Perencanaan kapasitas - Memahami persyaratan sumber daya beban kerja lokal untuk membantu Anda memigrasikan beban kerja Anda ke konfigurasi FSx untuk ONTAP yang lebih efisien. Anda juga dapat menggunakan wawasan ini untuk merencanakan kapan lebih banyak kinerja atau kapasitas akan diperlukan untuk fsX Anda untuk penyebaran ONTAP.

Untuk informasi selengkapnya tentang Cloud Insights, lihat NetApp Cloud Insights di NetApp Cloud Central.

Memantau FSx untuk sistem file ONTAP menggunakan Harvest dan Grafana

NetApp Harvest adalah alat open source untuk mengumpulkan metrik kinerja dan kapasitas dari sistem ONTAP, dan kompatibel dengan FSx untuk ONTAP. Anda dapat menggunakan Harvest with Grafana untuk solusi pemantauan open source.

Memulai Harvest dan Grafana

Bagian berikut merinci bagaimana Anda dapat mengatur dan mengonfigurasi Harvest dan Grafana untuk mengukur FSx Anda untuk kinerja sistem file ONTAP dan pemanfaatan kapasitas penyimpanan.

Anda dapat memantau Amazon FSx Anda untuk sistem file NetApp ONTAP dengan menggunakan Harvest dan Grafana. NetApp Harvest memantau pusat data ONTAP dengan mengumpulkan metrik kinerja, kapasitas, dan perangkat keras dari FSx untuk sistem file ONTAP. Grafana menyediakan dasbor tempat metrik Harvest yang dikumpulkan dapat ditampilkan.

Dasbor Harvest yang Didukung

Amazon FSx untuk NetApp ONTAP memperlihatkan kumpulan metrik yang berbeda dari ONTAP lokal. NetApp Oleh karena itu, hanya dasbor out-of-the-box Harvest berikut yang diberi tag saat ini didukung untuk `fsx` digunakan dengan FSx untuk ONTAP. Beberapa panel di dasbor ini mungkin kehilangan informasi yang tidak didukung.

- ONTAP: Kepatuhan
- ONTAP: Snapshot Perlindungan Data
- ONTAP: Keamanan
- ONTAP: SVM
- ONTAP: Volume

AWS CloudFormation Template

Untuk memulai, Anda dapat menerapkan AWS CloudFormation template yang secara otomatis meluncurkan instans Amazon EC2 yang menjalankan Harvest dan Grafana. Sebagai masukan ke AWS CloudFormation template, Anda menentukan `fsxadmin` pengguna dan titik akhir manajemen Amazon FSx untuk sistem file yang akan ditambahkan sebagai bagian dari penerapan ini. Setelah penerapan selesai, Anda dapat masuk ke dasbor Grafana untuk memantau sistem file Anda.

Solusi ini digunakan AWS CloudFormation untuk mengotomatiskan penerapan solusi Harvest dan Grafana. Template membuat instance Amazon EC2 Linux dan menginstal perangkat lunak Harvest dan Grafana. Untuk menggunakan solusi ini, unduh templat AWS CloudFormation fsx-ontap-harvest-grafana.template.

> **Note**
>
> Menerapkan solusi ini menimbulkan penagihan untuk layanan terkait. AWS Untuk informasi lebih lanjut, lihat halaman detail harga untuk layanan tersebut.

Jenis Instans Amazon EC2

Saat mengonfigurasi template, Anda memberikan jenis instans Amazon EC2. NetAppRekomendasi untuk ukuran instans tergantung pada berapa banyak sistem file yang Anda pantau dan jumlah metrik yang Anda pilih untuk dikumpulkan. Dengan konfigurasi default, untuk setiap 10 sistem file yang Anda pantau, NetApp rekomendasikan:

- CPU: 2 core
- Memori: 1 GB
- Disk: 500 MB (sebagian besar digunakan oleh file log)

Berikut ini adalah beberapa konfigurasi sampel dan jenis `t3` instance yang mungkin Anda pilih.

Sistem berkas	CPU	Disk	Jenis instans
Di bawah 10	2 inti	500 MB	`t3.micro`
10—40	4 inti	1000 MB	`t3.xlarge`

Sistem berkas	CPU	Disk	Jenis instans
40+	8 inti	2000 MB	`t3.2xlarge`

Untuk informasi selengkapnya tentang jenis instans Amazon EC2, lihat Instans tujuan umum di Panduan Pengguna Amazon EC2.

Aturan port instans

Saat menyiapkan instans Amazon EC2, pastikan port 3000 dan 9090 terbuka untuk lalu lintas masuk untuk grup keamanan tempat instans Amazon EC2 Harvest dan Grafana berada. Karena instance yang diluncurkan terhubung ke titik akhir melalui HTTPS, maka perlu menyelesaikan titik akhir, yang membutuhkan port 53 TCP/UDP untuk DNS. Selain itu, untuk mencapai titik akhir diperlukan port 443 TCP untuk HTTPS dan Akses Internet.

Prosedur penyebaran

Prosedur berikut mengkonfigurasi dan menyebarkan solusi Harvest/Grafana. Dibutuhkan sekitar lima menit untuk men-deploy. Sebelum memulai, Anda harus memiliki sistem file FSx untuk ONTAP yang berjalan di Amazon Virtual Private Cloud (Amazon VPC) di AWS akun Anda, dan informasi parameter untuk template yang tercantum di bawah ini. Untuk informasi selengkapnya tentang membuat sistem file, lihatMembuat fsX untuk sistem file ONTAP.

Untuk meluncurkan tumpukan solusi Harvest/Grafana

1. Unduh templat AWS CloudFormation fsx-ontap-harvest-grafana.template. Untuk informasi selengkapnya tentang membuat AWS CloudFormation tumpukan, lihat Membuat tumpukan di AWS CloudFormation konsol di Panduan AWS CloudFormation Pengguna.

   > **Note**
   >
   > Secara default, template ini diluncurkan di Wilayah AS Timur (Virginia N.) AWS . Anda harus meluncurkan solusi ini di Wilayah AWS tempat Amazon FSx tersedia. Untuk informasi selengkapnya, lihat titik akhir dan kuota Amazon FSx di.Referensi Umum AWS

2. Untuk Parameter, tinjau parameter untuk templat dan ubah sesuai kebutuhan sistem file Anda. Solusi ini menggunakan nilai default berikut.

Parameter	Default	Deskripsi
InstanceType	`t3.micro`	Jenis instans Amazon EC2. Berikut ini adalah jenis `t3` instance. • `t3.micro` • `t3.small` • `t3.medium` • `t3.large` • `t3.xlarge` • `t3.2xlarge` Untuk daftar lengkap nilai tipe instans Amazon EC2 yang diizinkan untuk parameter ini, lihat .template. fsx-ontap-harvest-grafana
KeyPair	Tidak ada nilai default	Key pair yang digunakan untuk mengakses instans Amazon EC2.
SecurityGroup	Tidak ada nilai default	ID grup Keamanan untuk Instans Harvest/Grafana. Pastikan port Inbound 3000 dan 9090, selain port 53 dan 443, terbuka dari klien yang ingin Anda gunakan untuk mengakses dasbor Grafana Anda.

Parameter	Default	Deskripsi
Jenis Subnet	Tidak ada nilai default	Tentukan jenis subnet, salah satu `public` atau`private`. Gunakan `public` subnet untuk sumber daya yang harus terhubung ke internet, dan subnet pribadi untuk sumber daya yang tidak akan terhubung ke internet. Untuk informasi selengkap nya, lihat Jenis subnet di Panduan Pengguna Amazon VPC.
Subnet	Tidak ada nilai default	Tentukan subnet yang sama dengan Amazon FSx Anda NetApp untuk subnet pilihan sistem file ONTAP. Anda dapat menemukan ID subnet Pilihan sistem file di konsol Amazon FSx, di tab Jaringan & keamanan pada halaman detail sistem file fsX untuk ONTAP
LatestLinuxAmiId	`/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2`	Versi terbaru dari Amazon Linux 2 AMI di berikan Wilayah AWS.

Parameter	Default	Deskripsi
SxEndTitik F	Tidak ada nilai default	Alamat IP titik akhir Manajemen sistem file. Anda dapat menemukan alamat IP titik akhir manajemen sistem file di konsol Amazon FSx, di tab Administrasi halaman detail sistem file fsX untuk ONTAP.
SecretName	Tidak ada nilai default	AWS Secrets Manager nama rahasia yang berisi kata sandi untuk `fsxadmin` pengguna sistem file. Ini adalah kata sandi yang Anda berikan saat Anda membuat sistem file.

3. Pilih Selanjutnya.
4. Untuk Opsi, pilih Selanjutnya.
5. Untuk Meninjau, tinjau dan konfirmasi pengaturan yang baru. Anda harus memilih kotak pengecekan yang menyatakan bahwa templat menghasilkan sumber daya IAM.
6. Pilih Buat untuk men-deploy tumpukan.

Anda dapat melihat status tumpukan di AWS CloudFormation konsol di kolom Status. Anda dapat melihat status CREATE_COMPLETE dalam waktu sekitar lima menit.

Masuk ke Grafana

Setelah penerapan selesai, gunakan browser Anda untuk masuk ke dasbor Grafana di IP dan port 3000 instans Amazon EC2:

```
http://EC2_instance_IP:3000
```

Saat diminta, gunakan nama pengguna default Grafana `admin` () dan kata sandi `pass` (). Kami menyarankan Anda mengubah kata sandi Anda segera setelah Anda masuk.

Untuk informasi lebih lanjut, lihat halaman NetApp Harvest di GitHub.

Pemecahan Masalah Panen dan Grafana

Jika Anda menemukan data yang hilang yang disebutkan di dasbor Harvest dan Grafana atau mengalami kesulitan dalam mengatur Harvest dan Grafana dengan FSx untuk ONTAP, periksa topik berikut untuk solusi potensial.

Topik

Dasbor SVM dan volume kosong

Jika AWS CloudFormation tumpukan berhasil diterapkan dan dapat menghubungi Grafana tetapi SVM dan dasbor volume kosong, gunakan prosedur berikut untuk memecahkan masalah lingkungan Anda. Anda akan memerlukan akses SSH ke instans Amazon EC2 tempat Harvest dan Grafana digunakan.

1. SSH ke instans Amazon EC2 tempat klien Harvest dan Grafana Anda berjalan.

   ```
   [~]$ ssh ec2-user@ec2_ip_address
   ```

2. Gunakan perintah berikut untuk membuka `harvest.yml` file dan:

   - Verifikasi bahwa entri telah dibuat untuk FSx Anda untuk instans ONTAP sebagai. `Cluster-2`
   - Verifikasi bahwa entri untuk nama pengguna dan kata sandi cocok dengan `fsxadmin` kredensi Anda.

   ```
   [ec2-user@ip-ec2_ip_address ~]$ sudo cat /home/ec2-user/harvest_install/harvest/
   harvest.yml
   ```

3. Jika bidang kata sandi kosong, buka file di editor dan perbarui dengan `fsxadmin` kata sandi, sebagai berikut:

   ```
   [ec2-user@ip-ec2_ip_address ~]$ sudo vi /home/ec2-user/harvest_install/harvest/
   harvest.yml
   ```

4. Pastikan kredenal `fsxadmin` pengguna disimpan di Secrets Manager dalam format berikut untuk penerapan di masa mendatang, ganti *`fsxadmin_password`* dengan kata sandi Anda.

```
{"username" : "fsxadmin", "password" : "fsxadmin_password"}
```

CloudFormation tumpukan digulung kembali setelah batas waktu

Jika Anda tidak dapat menyebarkan CloudFormation tumpukan dengan sukses dan bergulir kembali dengan kesalahan, gunakan prosedur berikut untuk menyelesaikan masalah. Anda akan memerlukan akses SSH ke instans EC2 yang digunakan oleh tumpukan. CloudFormation

1. Pasang kembali CloudFormation tumpukan, pastikan rollback otomatis dinonaktifkan.
2. SSH ke instans Amazon EC2 tempat klien Harvest dan Grafana Anda berjalan.

```
[~]$ ssh ec2-user@ec2_ip_address
```

3. Verfy bahwa wadah docker berhasil dimulai menggunakan perintah berikut.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo docker ps
```

Dalam tanggapan Anda akan melihat lima kontainer sebagai berikut:

```
CONTAINER ID   IMAGE                    COMMAND                  CREATED
 STATUS                          PORTS                     NAMES
6b9b3f2085ef   rahulguptajss/harvest   "bin/poller --config…"   8 minutes ago
 Restarting (1) 20 seconds ago                             harvest_cluster-2
3cf3e3623fde   rahulguptajss/harvest   "bin/poller --config…"   8 minutes ago   Up
 About a minute                                            harvest_cluster-1
708f3b7ef6f8   grafana/grafana         "/run.sh"                8 minutes ago   Up
 8 minutes                   0.0.0.0:3000->3000/tcp   harvest_grafana
0febee61cab7   prom/alertmanager       "/bin/alertmanager -…"   8
 minutes ago   Up 8 minutes                    0.0.0.0:9093->9093/tcp
 harvest_prometheus_alertmanager
1706d8cd5a0c   prom/prometheus         "/bin/prometheus --c…"   8 minutes ago   Up
 8 minutes                   0.0.0.0:9090->9090/tcp   harvest_prometheus
```

4. Jika wadah docker tidak berjalan, periksa kegagalan dalam `/var/log/cloud-init-output.log` file sebagai berikut.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo cat /var/log/cloud-init-output.log
     PLAY [Manage Harvest]
 ************************************************************

TASK [Gathering Facts] ************************************************************
ok: [localhost]

TASK [Verify images] ************************************************************
failed: [localhost] (item=prom/prometheus) => {"ansible_loop_var": "item",
 "changed": false, "item": "prom/prometheus",
"msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}
failed: [localhost] (item=prom/alertmanager) => {"ansible_loop_var": "item",
 "changed": false, "item": "prom/alertmanage
r", "msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104,
'Connection reset by peer'))"}
failed: [localhost] (item=rahulguptajss/harvest) => {"ansible_loop_var": "item",
 "changed": false, "item": "rahulguptajs
s/harvest", "msg": "Error connecting: Error while fetching server API version:
 ('Connection aborted.', ConnectionResetEr
ror(104, 'Connection reset by peer'))"}
failed: [localhost] (item=grafana/grafana) => {"ansible_loop_var": "item",
 "changed": false, "item": "grafana/grafana",
"msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}

PLAY RECAP ************************************************************************
localhost                  : ok=1    changed=0    unreachable=0    failed=1
 skipped=0    rescued=0    ignored=0
```

5. Jika ada kegagalan, jalankan perintah berikut untuk menyebarkan kontainer Harvest dan Grafana.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo su
     [ec2-user@ip-ec2_ip_address ~]$ cd /home/ec2-user/harvest_install
     [ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
 manage_harvest.yml
     [ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
 manage_harvest.yml --tags api
```

6. Validasi kontainer yang dimulai dengan sukses dengan menjalankan sudo docker ps dan menghubungkan ke URL Harvest dan Grafana Anda.

Logging FSx untuk Panggilan API ONTAP denganAWS CloudTrail

Amazon FSx terintegrasi denganAWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atauAWSlayanan di Amazon FSx. CloudTrail menangkap semua panggilan API Amazon FSx untuk NetApp ONTAP sebagai peristiwa. Panggilan yang tertangkap meliputi panggilan dari konsol Amazon FSx dan dari panggilan kode ke operasi API Amazon FSx.

Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman berkelanjutan CloudTrail peristiwa ke bucket Amazon S3, termasuk peristiwa untuk Amazon FSx. Jika Anda tidak mengonfigurasi jejak, Anda masih bisa melihat kejadian terbaru di CloudTrail konsol diRiwayat peristiwa. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke Amazon FSx. Anda juga dapat menentukan alamat IP untuk membuat permintaan, siapa yang membuat permintaan, kapan permintaan dibuat, dan detail tambahan.

Untuk mempelajari lebih lanjut tentang CloudTrail, lihat Panduan Pengguna AWS CloudTrail.

Informasi Amazon FSx di CloudTrail

CloudTrail diaktifkan pada akun AWS Anda saat Anda membuat akun tersebut. Ketika aktivitas API terjadi di Amazon FSx, aktivitas tersebut dicatat di CloudTrail acara bersama dengan lainnyaAWSPeristiwa layanan diRiwayat peristiwa. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun AWS Anda. Untuk informasi selengkapnya, lihatMelihat peristiwa dengan CloudTrail Riwayat peristiwa.

Untuk catatan peristiwa yang sedang berlangsung di akun AWS Anda, termasuk peristiwa untuk Amazon FSx, buat jejak. SEBUAHjejakmenyalakan CloudTrail mengirimkan berkas log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di dalam konsol tersebut, jejak diterapkan ke semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah AWS di partisi AWS dan mengirimkan berkas log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi lainnyaAWSlayanan untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan di CloudTrail log. Untuk informasi lebih lanjut, lihat topik berikut di Panduan Pengguna AWS CloudTrail:

- Membuat jejak untuk AndaAkun AWS
- AWSIntegrasi layanan dengan CloudTrail Beberapa catatan

- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima CloudTrail berkas log dari beberapa wilayahdanMenerima berkas log CloudTrail dari beberapa akun

Semua Panggilan API Amazon FSx for Lustre dicatat oleh CloudTrail. Misalnya, panggilan ke`CreateFileSystem`dan`TagResource`operasi menghasilkan entri dalam CloudTrail berkas log.

Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut:

- Bahwa permintaan dibuat dengan kredensial pengguna root atau pengguna AWS Identity and Access Management (IAM).
- Bahwa permintaan tersebut dibuat dengan kredensial keamanan sementara untuk peran atau pengguna gabungan.
- Apakah permintaan dibuat oleh layanan AWS yang lain.

Untuk informasi selengkapnya, lihat elemen userIdentity CloudTrail di Panduan Pengguna AWS CloudTrail.

Memahami entri Berkas Log Amazon FSx

SEBUAHjejakadalah konfigurasi yang mengaktifkan pengiriman peristiwa sebagai berkas log ke bucket Amazon S3 yang Anda tentukan. CloudTrail File log berisi satu atau beberapa entri log. Sesiperistiwamewakili satu permintaan dari sumber mana pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail File log bukan merupakan jejak tumpukan terurut dari panggilan API publik, sehingga berkas tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan CloudTrail entri log yang menunjukkan`TagResource`operasi ketika tag untuk sistem file dibuat dari konsol.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": “111122223333”,
        "arn": "arn:aws:sts::111122223333:root”,
        "accountId": “111122223333”,
```

```
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE”,
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T22:36:07Z"
            }
        }
    },
    "eventTime": "2018-11-14T22:36:07Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": “192.0.2.0”,
    "userAgent": “console.amazonaws.com”,
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789”
    },
    "responseElements": null,
    "requestID": “aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51”,
    "eventID": “bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p”,
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": “111122223333”
}
```

Contoh berikut menunjukkan CloudTrail entri log yang menunjukkan`UntagResource`ketika tag untuk sistem file dibuat dari konsol.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": "111122223333",
        "arn": "arn:aws:sts::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T23:40:54Z"
            }
        }
```

```
    },
    "eventTime": "2018-11-14T23:40:54Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "UntagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789"
    },
    "responseElements": null,
    "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
    "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": "111122223333"
}
```

Kuota

Berikut ini, Anda dapat mengetahui tentang kuota saat bekerja dengan Amazon FSx NetApp untuk ONTAP.

Topik

Kuota yang dapat Anda tingkatkan

Berikut ini adalah kuota untuk Amazon FSx untuk ONTAP NetApp untuk Akun AWS masing-masing, Wilayah AWS per, yang dapat Anda tingkatkan.

Sumber daya	Default	Deskripsi
ONTAPsistem berkas	100	Jumlah maksimum Amazon FSx untuk sistem file NetApp ONTAP yang dapat Anda buat di akun ini.
ONTAPKapasitas penyimpanan SSD	524,288	Jumlah maksimum kapasitas penyimpanan SSD (dalam GiB) untuk semua Amazon FSx untuk sistem file NetApp ONTAP yang dapat Anda miliki di akun ini.
ONTAPkapasitas throughput	10,240	Jumlah maksimum kapasitas throughput (dalam MBps) untuk semua Amazon FSx untuk sistem file NetApp ONTAP yang dapat Anda miliki di akun ini.

Sumber daya	Default	Deskripsi
ONTAPSSD IOPS	1.000.000	Jumlah maksimum SSD IOPS untuk semua Amazon FSx NetApp untuk sistem file ONTAP yang dapat Anda miliki di akun ini.
ONTAPbackup per sistem file	10.000	Jumlah maksimum pencadangan volume yang dimulai pengguna untuk semua Amazon FSx NetApp untuk sistem file ONTAP yang dapat Anda miliki di akun ini.

Untuk meminta peningkatan kuota

1. Buka AWS Supporthalaman, masuk jika perlu, lalu pilih Buat kasus.
2. Untuk Buat kasus, pilih Support akun dan penagihan.
3. Di panel Detail kasus buat entri berikut:
   - Untuk Jenis, pilih Akun.
   - Untuk Kategori pilih Masalah Akun lainnya.
   - Untuk Subjek masukkan **`Amazon FSx for NetApp ONTAP service limit increase request`**.
   - Sediakan detail Deskripsi permintaan Anda, termasuk:
     - Kuota FSx yang Anda inginkan meningkat, dan nilai yang Anda inginkan meningkat, jika diketahui.
     - Alasan mengapa Anda mencari peningkatan kuota.
     - ID sistem file dan wilayah untuk setiap sistem file yang Anda minta peningkatan.
4. Berikan Opsi kontak pilihan Anda dan pilih Kirim.

Kuota sumber daya untuk setiap sistem file

Tabel berikut mencantumkan kuota di Amazon FSx NetApp untuk sumber daya ONTAP untuk setiap sistem file dalam file. Wilayah AWS

Sumber daya	Batas per sistem file
Kapasitas penyimpanan SSD minimum	1.024 GiB per pasangan ketersedi aan tinggi (HA)
Kapasitas penyimpanan SSD maksimum	• Scale-out: 512 TiB per pasangan HA, hingga 1 piB • Peningkatan skala: 192 TiB
IOPS SSD maksimum	Skala-keluar: • 200.000 per pasangan HA (hingga 12 pasang) Peningkatan skala: • 160.000 di Wilayah AS Timur (Ohio), Wilayah AS Timur (Virginia N.), Wilayah AS Barat (Oregon), dan Eropa (Irlandia) • 80.000 di semua Wilayah AWS tempat lain di mana FSx untuk ONTAP tersedia
Kapasitas throughput minimum	• Penskalaan: 3.072 MBps per pasangan HA • Peningkatan skala: 128 MBps
Kapasitas throughput maksimum	Skala-keluar: • 73.728 MBps 1 Peningkatan skala:

Sumber daya	Batas per sistem file
	• 4.096 MBps [2] di Wilayah AS Timur (Ohio), Wilayah AS Timur (Virginia N.), Wilayah AS Barat (Oregon), dan Eropa (Irlandia) • 2.048 MBps di semua tempat lain di mana Wilayah AWS FSx untuk ONTAP tersedia
Jumlah volume maksimum	• Skala-out: 1.000 • Peningkatan skala: 500
Jumlah snapshot maksimum	1.023 per volume [3]
Jumlah maksimum backup	4.091 per volume [4]
Jumlah maksimum SVM	Skala-keluar: • 5 Peningkatan skala: • 6 (kapasitas throughput 128 MBps) • 6 (kapasitas throughput 256 MBps) • 14 (kapasitas throughput 512 MBps) • 14 (kapasitas throughput 1.024 MBps) • 24 (kapasitas throughput 2.048 MBps) • 24 (kapasitas throughput 4.096 MBps)
Jumlah maksimum tag	50

Sumber daya	Batas per sistem file
Periode penyimpanan maksimum untuk cadangan otomatis	90 hari
Periode retensi maksimum untuk pencadangan yang dimulai pengguna	Tidak ada batas retensi
Jumlah maksimum rute yang didukung per sistem file	50 [5]

Note

[1] Pada sistem file scale-out dengan 12 pasang HA (6.144 MBps per pasangan HA). Untuk informasi selengkapnya, lihat Pasangan ketersediaan tinggi (HA).

[2] Untuk menyediakan kapasitas throughput 4 GBps, sistem file scale-up FSx untuk ONTAP Anda memerlukan konfigurasi IOPS SSD maksimum (160.000) dan minimal 5.120 GiB kapasitas penyimpanan SSD yang didukung. Wilayah AWS Untuk informasi lebih lanjut tentang yang Wilayah AWS mendukung kapasitas throughput 4.096 MBps, lihat. Dampak kapasitas throughput terhadap performa

[3] Anda dapat menyimpan hingga 1.023 snapshot per volume kapan saja. Setelah Anda mencapai batas ini, Anda harus menghapus snapshot yang ada sebelum snapshot baru volume Anda dapat dibuat.

[4] Anda dapat menyimpan hingga 4.091 cadangan per volume kapan saja. Setelah Anda mencapai batas ini, Anda harus menghapus cadangan yang ada sebelum cadangan baru volume Anda dapat dibuat.

[5] Anda dapat mengonfigurasi hingga 50 rute per sistem file kapan saja. Setelah Anda mencapai batas ini, Anda harus menghapus rute yang ada sebelum rute baru dapat dikonfigurasi. Jumlah rute yang dimiliki sistem file Anda ditentukan oleh jumlah SVM yang dimilikinya dan jumlah tabel rute yang terkait dengannya. Anda dapat menentukan jumlah rute yang ada ke sistem file menggunakan persamaan berikut: (1 + jumlah SVM dalam sistem file) * (tabel rute yang terkait dengan sistem file).

Memecahkan Masalah Amazon FSx untuk ONTAP NetApp

Gunakan bagian berikut untuk membantu memecahkan masalah yang Anda miliki dengan FSx untuk ONTAP.

Topik

Sistem file Multi-AZ saya dalam keadaan **`MISCONFIGURED`**

Ada sejumlah penyebab potensial untuk sistem file berada dalam `MISCONFIGURED` keadaan, masing-masing dengan resolusi mereka sendiri, sebagai berikut.

Topik

Akun pemilik VPC telah menonaktifkan berbagi VPC multi-AZ

Sistem file multi-AZ yang dibuat oleh peserta Akun AWS dalam subnet VPC bersama akan masuk ke `MISCONFIGURED` status karena salah satu alasan berikut:

- Akun pemilik yang membagikan subnet VPC telah menonaktifkan dukungan berbagi VPC multi-AZ untuk FSx untuk sistem file ONTAP.
- Akun pemilik tidak membagikan subnet VPC.

Jika akun pemilik tidak membagikan subnet VPC, Anda akan melihat pesan berikut di konsol untuk sistem file tersebut:

```
The vpc ID vpc-012345abcde does not exist
```

Anda perlu menghubungi akun pemilik yang membagikan subnet VPC dengan Anda untuk mengatasi masalah tersebut. Untuk informasi lebih lanjut, lihat Membuat fsX untuk sistem file ONTAP di subnet bersama untuk informasi lebih lanjut.

Anda tidak dapat membuat SVM baru pada sistem file Multi-AZ

Untuk sistem file multi-AZ yang dibuat oleh peserta Akun AWS dalam VPC bersama, Anda tidak akan dapat membuat SVM baru karena salah satu alasan berikut:

- Akun pemilik yang membagikan subnet VPC telah menonaktifkan dukungan berbagi VPC multi-AZ untuk FSx untuk sistem file ONTAP.
- Akun pemilik tidak membagikan subnet VPC.

Anda perlu menghubungi akun pemilik yang membagikan subnet VPC dengan Anda untuk mengatasi masalah tersebut. Untuk informasi lebih lanjut, lihat Membuat fsX untuk sistem file ONTAP di subnet bersama untuk informasi lebih lanjut.

Anda tidak dapat mengakses sistem file Anda

Ada beberapa kemungkinan penyebab Anda tidak dapat mengakses sistem file Anda, masing-masing memiliki penyelesaian masalah sendiri, sebagai berikut.

Topik

- Elastic network interface sistem file telah dimodifikasi atau dihapus
- Alamat IP Elastis yang dilampirkan ke elastic network interface sistem file telah dihapus
- Grup keamanan VPC sistem file tidak memiliki aturan masuk yang diperlukan
- Grup keamanan VPC instans komputasi tidak memiliki aturan keluar yang diperlukan
- Subnet instance komputasi tidak menggunakan tabel rute apa pun yang terkait dengan sistem file Anda
- Amazon FSx tidak dapat memperbarui tabel rute untuk sistem file Multi-AZ yang dibuat menggunakan AWS CloudFormation
- Tidak dapat mengakses sistem file melalui iSCSI dari klien di VPC lain
- Akun pemilik tidak membagikan subnet VPC

- Tidak dapat mengakses sistem file melalui NFS, SMB, CLI ONTAP, atau ONTAP REST API dari klien di VPC lain atau lokal

Elastic network interface sistem file telah dimodifikasi atau dihapus

Anda tidak boleh memodifikasi atau menghapus salah satu antarmuka jaringan elastis sistem file. Memodifikasi atau menghapus antarmuka jaringan dapat menyebabkan hilangnya koneksi permanen antara virtual private cloud (VPC) dan sistem file Anda. Buat sistem file baru, dan jangan memodifikasi atau menghapus antarmuka jaringan Amazon FSx. Untuk informasi selengkapnya, lihat Kontrol Akses Sistem File dengan Amazon VPC.

Alamat IP Elastis yang dilampirkan ke elastic network interface sistem file telah dihapus

Amazon FSx tidak support sistem file akses dari internet publik. Amazon FSx secara otomatis melepaskan alamat IP Elastic yang merupakan alamat IP publik yang dapat dijangkau dari Internet yang dilampirkan ke antarmuka network elastis sistem file. Untuk informasi selengkapnya, lihat Klien yang didukung.

Grup keamanan VPC sistem file tidak memiliki aturan masuk yang diperlukan

Tinjau aturan masuk yang ditentukan dalam Grup keamanan Amazon VPC, dan pastikan bahwa grup keamanan yang terkait dengan sistem file Anda memiliki aturan masuk yang sesuai.

Grup keamanan VPC instans komputasi tidak memiliki aturan keluar yang diperlukan

Tinjau aturan keluar yang ditentukan dalam Grup keamanan Amazon VPC, dan pastikan bahwa grup keamanan yang terkait dengan instans komputasi Anda memiliki aturan keluar yang sesuai.

Subnet instance komputasi tidak menggunakan tabel rute apa pun yang terkait dengan sistem file Anda

FSx untuk ONTAP membuat titik akhir untuk mengakses sistem file Anda dalam tabel rute VPC. Kami menyarankan Anda mengonfigurasi sistem file Anda untuk menggunakan semua tabel rute VPC yang terkait dengan subnet tempat klien Anda berada. Secara default, Amazon FSx menggunakan tabel

rute utama VPC Anda. Anda dapat secara opsional menentukan satu atau beberapa tabel rute untuk Amazon FSx untuk digunakan saat Anda membuat sistem file Anda.

Jika Anda dapat melakukan ping ke titik akhir Intercluster sistem file Anda tetapi tidak dapat melakukan ping ke titik akhir Manajemen sistem file Anda (lihat Sumber daya sistem file untuk informasi lebih lanjut), klien Anda kemungkinan tidak berada dalam subnet yang terkait dengan salah satu tabel rute sistem file Anda. Untuk mengakses sistem file Anda, kaitkan salah satu tabel rute sistem file Anda dengan subnet klien Anda. Untuk informasi tentang memperbarui tabel rute Amazon VPC sistem file Anda, lihat. Memperbarui sistem file

Amazon FSx tidak dapat memperbarui tabel rute untuk sistem file Multi-AZ yang dibuat menggunakan AWS CloudFormation

Amazon FSx mengelola tabel rute VPC untuk sistem file multi-AZ menggunakan otentikasi berbasis tag. Tabel rute ini ditandai dengan`Key: AmazonFSx; Value: ManagedByAmazonFSx`.
Saat membuat atau memperbarui FSx untuk sistem file Multi-AZ ONTAP menggunakan AWS CloudFormation kami sarankan Anda menambahkan tag secara manual. `Key: AmazonFSx; Value: ManagedByAmazonFSx`

Jika Anda tidak dapat menjangkau sistem file Multi-AZ Anda, periksa untuk melihat apakah tabel rute VPC yang terkait dengan sistem file ditandai. `Key: AmazonFSx; Value: ManagedByAmazonFSx` Jika tidak, maka Amazon FSx tidak dapat memperbarui tabel rute tersebut untuk merutekan alamat IP mengambang dari manajemen dan port data ke server file aktif ketika peristiwa failover terjadi. Untuk informasi tentang memperbarui tabel rute Amazon VPC sistem file Anda, lihat. Memperbarui sistem file

Tidak dapat mengakses sistem file melalui iSCSI dari klien di VPC lain

Untuk mengakses sistem file melalui protokol Internet Small Computer Systems Interface (iSCSI) dari klien di VPC lain, Anda dapat mengonfigurasi peering VPC Amazon atau AWS Transit Gateway antara VPC yang terkait dengan sistem file Anda dan VPC tempat klien Anda berada. Untuk informasi selengkapnya, lihat Membuat dan menerima koneksi peering VPC di panduan Amazon Virtual Private Cloud.

Akun pemilik tidak membagikan subnet VPC

Jika Anda membuat sistem file di subnet VPC yang telah dibagikan dengan Anda, akun pemilik mungkin telah membatalkan pembagian subnet VPC.

Jika akun pemilik tidak membagikan subnet VPC, Anda akan melihat pesan berikut di konsol untuk sistem file tersebut:

```
The vpc ID vpc-012345abcde does not exist
```

Anda harus menghubungi akun pemilik sehingga mereka dapat berbagi kembali subnet dengan Anda.

Tidak dapat mengakses sistem file melalui NFS, SMB, CLI ONTAP, atau ONTAP REST API dari klien di VPC lain atau lokal

Untuk mengakses sistem file melalui Network File System (NFS), Server Message Block (SMB), atau NetApp ONTAP CLI dan REST API dari klien di VPC lain atau di tempat, Anda harus mengonfigurasi perutean menggunakan AWS Transit Gateway antara VPC yang terkait dengan sistem file Anda dan jaringan tempat klien Anda berada. Untuk informasi selengkapnya, lihat Mengakses data.

Anda tidak dapat bergabung dengan mesin virtual penyimpanan (SVM) ke Active Directory

Jika Anda tidak dapat bergabung dengan SVM ke Active Directory (AD), tinjau Bergabung dengan SVM ke Microsoft Active Directory terlebih dahulu. Masalah umum yang mencegah SVM bergabung ke Direktori Aktif Anda tercantum di bagian berikut, termasuk pesan kesalahan yang dihasilkan untuk setiap keadaan.

Topik

- Nama SVM NetBIOS sama dengan nama NetBIOS untuk domain rumah.
- SVM sudah bergabung dengan Active Directory lain
- Amazon FSx tidak dapat terhubung ke pengontrol domain Direktori Aktif Anda karena nama NetBios SVM sudah digunakan
- Amazon FSx tidak dapat berkomunikasi dengan pengontrol domain Direktori Aktif
- Amazon FSx tidak dapat terhubung ke Direktori Aktif Anda karena persyaratan port yang tidak terpenuhi atau izin akun layanan
- Amazon FSx tidak dapat terhubung ke pengontrol domain Direktori Aktif karena kredensyal akun layanan tidak valid
- Amazon FSx tidak dapat terhubung ke pengontrol domain Direktori Aktif karena kredensyal akun layanan tidak mencukupi

- Amazon FSx tidak dapat berkomunikasi dengan server DNS Direktori Aktif atau pengontrol domain
- Amazon FSx tidak dapat berkomunikasi dengan Active Directory karena nama domain Active Directory tidak valid.
- Akun layanan tidak dapat mengakses grup administrator yang ditentukan dalam konfigurasi SVM Active Directory
- Amazon FSx tidak dapat terhubung ke pengontrol domain Direktori Aktif karena unit organisasi yang ditentukan tidak ada atau tidak dapat diakses

Nama SVM NetBIOS sama dengan nama NetBIOS untuk domain rumah.

Bergabung dengan SVM ke Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

Amazon FSx tidak dapat membuat koneksi dengan Direktori Aktif Anda. Ini karena nama server yang Anda tentukan adalah nama NetBIOS dari domain rumah. Untuk memperbaiki masalah ini, pilih nama NetBIOS untuk SVM Anda yang berbeda dari nama NetBIOS dari domain rumah. Kemudian coba kembali untuk bergabung dengan SVM Anda ke Active Directory Anda.

Untuk mengatasi masalah ini, ikuti prosedur yang dijelaskan Bergabung dengan SVM ke Active Directory menggunakan AWS Management Console, AWS CLI dan API untuk mencoba kembali bergabung dengan SVM Anda ke AD Anda. Pastikan Anda menggunakan nama NetBIOS untuk SVM Anda yang berbeda dari nama NetBIOS dari domain home Active Directory.

SVM sudah bergabung dengan Active Directory lain

Bergabung dengan SVM ke Active Directory gagal dengan pesan galat berikut:

Amazon FSx tidak dapat membuat sambungan ke Direktori Aktif Anda. Ini karena SVM sudah bergabung ke domain. Untuk menggabungkan SVM ini ke domain lain, Anda dapat menggunakan ONTAP CLI atau REST API untuk memutuskan sambungan SVM ini dari Active Directory. Kemudian coba kembali untuk bergabung dengan SVM Anda ke Active Directory yang berbeda.

Untuk mengatasi masalah ini, lakukan hal berikut:

1. Gunakan CLI NetApp ONTAP untuk memutuskan sambungan SVM dari Active Directory saat ini. Untuk informasi selengkapnya, lihat Berhenti bergabung dengan Active Directory dari SVM Anda menggunakan ONTAP NetApp CLI.

2. Ikuti prosedur yang dijelaskan Bergabung dengan SVM ke Active Directory menggunakan AWS Management Console, AWS CLI dan API untuk mencoba kembali bergabung dengan SVM Anda ke AD baru.

Amazon FSx tidak dapat terhubung ke pengontrol domain Direktori Aktif Anda karena nama NetBios SVM sudah digunakan

Membuat SVM yang bergabung dengan AD yang dikelola sendiri gagal dengan pesan galat berikut:

Amazon FSx tidak dapat membuat koneksi dengan Direktori Aktif Anda. Ini karena nama NetBIOS (komputer) yang Anda tentukan sudah digunakan di Active Directory Anda. Untuk memperbaiki masalah ini, pilih nama NetBIOS untuk SVM Anda yang tidak digunakan di Direktori Aktif Anda., tentukan NetBIOS (komputer) Kemudian coba kembali untuk bergabung dengan SVM Anda ke Direktori Aktif Anda.

Untuk mengatasi masalah ini, ikuti prosedur yang dijelaskan Bergabung dengan SVM ke Active Directory menggunakan AWS Management Console, AWS CLI dan API untuk mencoba kembali bergabung dengan SVM Anda ke AD Anda. Pastikan Anda menggunakan nama NetBIOS untuk SVM Anda yang unik dan belum digunakan di Direktori Aktif Anda.

Amazon FSx tidak dapat berkomunikasi dengan pengontrol domain Direktori Aktif

Bergabung dengan SVM ke AD yang dikelola sendiri gagal dengan pesan galat berikut:

Amazon FSx tidak dapat berkomunikasi dengan Active Directory Anda. Untuk memperbaiki masalah ini, pastikan lalu lintas jaringan diizinkan antara Amazon FSx dan pengontrol domain Anda. Kemudian coba kembali untuk bergabung dengan SVM Anda ke Active Directory Anda.

Untuk mengatasi masalah ini, lakukan solusi berikut:

1. Tinjau persyaratan yang dijelaskan dalamPersyaratan konfigurasi jaringan, dan buat perubahan yang diperlukan untuk mengaktifkan komunikasi jaringan antara Amazon FSx dan AD Anda.
2. Setelah Amazon FSx dapat berkomunikasi dengan iklan Anda, ikuti prosedur yang dijelaskan Bergabung dengan SVM ke Active Directory menggunakan AWS Management Console, AWS CLI dan API dan coba kembali menggabungkan SVM Anda ke AD Anda.

Amazon FSx tidak dapat terhubung ke Direktori Aktif Anda karena persyaratan port yang tidak terpenuhi atau izin akun layanan

Bergabung dengan SVM ke AD yang dikelola sendiri gagal dengan pesan galat berikut:

Amazon FSx tidak dapat membuat koneksi dengan Direktori Aktif Anda. Hal ini disebabkan oleh persyaratan port untuk Direktori Aktif Anda tidak terpenuhi, atau akun layanan yang disediakan tidak memiliki izin untuk bergabung dengan mesin virtual penyimpanan ke domain dengan unit organisasi yang ditentukan. Untuk memperbaiki masalah ini, perbarui konfigurasi Direktori Aktif mesin virtual penyimpanan Anda setelah menyelesaikan masalah izin apa pun dengan port dan akun layanan, seperti yang direkomendasikan dalam panduan pengguna Amazon FSx.

Untuk mengatasi masalah ini, lakukan solusi berikut:

1. Tinjau persyaratan yang dijelaskan dalamPersyaratan konfigurasi jaringan, dan buat perubahan yang diperlukan untuk memenuhi persyaratan jaringan dan memastikan komunikasi diaktifkan pada port yang diperlukan
2. Tinjau persyaratan akun layanan yang dijelaskan dalamPersyaratan akun layanan Direktori Aktif. Pastikan akun layanan memiliki izin yang didelegasikan yang diperlukan untuk menggabungkan SVM Anda ke domain AD menggunakan unit organisasi yang ditentukan.
3. Setelah Anda membuat perubahan pada izin port atau akun layanan, ikuti prosedur yang dijelaskan Bergabung dengan SVM ke Active Directory menggunakan AWS Management Console, AWS CLI dan API dan coba kembali bergabung dengan SVM Anda ke AD Anda.

Amazon FSx tidak dapat terhubung ke pengontrol domain Direktori Aktif karena kredensyal akun layanan tidak valid

Bergabung dengan SVM ke Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

Amazon FSx tidak dapat membuat sambungan dengan pengontrol domain Direktori Aktif karena kredensyal akun layanan yang diberikan tidak valid. Untuk memperbaiki masalah ini, perbarui konfigurasi Active Directory mesin virtual penyimpanan Anda dengan akun layanan yang valid.

Untuk mengatasi masalah ini, gunakan prosedur yang dijelaskan Memperbarui konfigurasi SVM Active Directory yang ada menggunakan AWS Management Console, AWS CLI, dan API untuk memperbarui kredensyal akun layanan SVM. Saat memasukkan nama pengguna akun layanan, pastikan untuk hanya menyertakan nama pengguna (misalnya,`ServiceAcct`), dan jangan

menyertakan awalan domain apa pun (misalnya,`corp.com\ServiceAcct`) atau akhiran domain (misalnya,`ServiceAcct@corp.com`). Jangan gunakan nama terhormat (DN) saat memasukkan nama pengguna akun layanan (misalnya,`CN=ServiceAcct,OU=example,DC=corp,DC=com`).

Amazon FSx tidak dapat terhubung ke pengontrol domain Direktori Aktif karena kredensyal akun layanan tidak mencukupi

Bergabung dengan SVM ke Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

Amazon FSx tidak dapat membuat koneksi dengan pengontrol domain Direktori Aktif Anda. Ini karena persyaratan port untuk Direktori Aktif belum terpenuhi, atau akun layanan yang diberikan tidak memiliki izin untuk bergabung dengan mesin virtual penyimpanan ke domain dengan unit organisasi yang ditentukan.

Untuk mengatasi masalah ini, pastikan Anda telah mendelegasikan izin yang diperlukan ke akun layanan yang Anda berikan. Akun layanan harus mampu membuat dan menghapus objek komputer di OU di domain yang Anda gabungkan dengan sistem file. Untuk memiliki izin, Akun layanan juga setidaknya perlu untuk melakukan hal berikut:

- Atur ulang kata sandi
- Batasi akun dari membaca dan menulis data
- Kemampuan tervalidasi untuk menulis ke nama host DNS
- Kemampuan tervalidasi untuk menulis ke nama utama layanan
- Kemampuan untuk membuat dan menghapus objek komputer
- Kemampuan tervalidasi untuk membaca dan menulis Pembatasan Akun

Untuk informasi selengkapnya tentang membuat akun layanan dengan izin yang benar, lihat Persyaratan akun layanan Direktori Aktif danMendelegasikan izin ke akun layanan Amazon FSx Anda.

Amazon FSx tidak dapat berkomunikasi dengan server DNS Direktori Aktif atau pengontrol domain

Bergabung dengan SVM ke Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

Amazon FSx tidak dapat berkomunikasi dengan Active Directory Anda. Ini karena Amazon FSx tidak dapat menjangkau server DNS yang disediakan atau pengontrol domain untuk domain Anda. Untuk

memperbaiki masalah ini, perbarui konfigurasi Active Directory mesin virtual penyimpanan Anda dengan server DNS yang valid dan konfigurasi jaringan yang memungkinkan lalu lintas mengalir dari mesin virtual penyimpanan ke pengontrol domain.

Untuk mengatasi masalah ini, gunakan prosedur berikut:

1. Jika hanya beberapa pengontrol domain di Active Directory yang dapat dijangkau, misalnya karena keterbatasan geografis atau firewall, Anda dapat menambahkan pengontrol domain pilihan. Dengan menggunakan opsi ini, Amazon FSx mencoba menghubungi pengontrol domain pilihan. Tambahkan pengontrol domain pilihan menggunakan perintah `vserver cifs domain preferred-dc add` NetApp ONTAP CLI, sebagai berikut:

   a. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen Amazon fsX NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *`management_endpoint_ip`* dengan alamat IP port manajemen sistem file.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Untuk informasi selengkapnya, lihat Mengelola sistem file dengan ONTAP CLI.

   b. Masukkan perintah berikut, di mana:

   - `-vserver vserver_name`menentukan nama mesin virtual penyimpanan (SVM).
   - `-domain domain_name`menentukan nama Active Directory (FQDN) yang sepenuhnya memenuhi syarat dari domain yang menjadi milik pengontrol domain tertentu.
   - `-preferred-dc IP_address,…` menentukan satu atau lebih alamat IP dari pengontrol domain pilihan, sebagai daftar yang dibatasi koma, dalam urutan preferensi.

   ```
   FsxId123456789::> vserver cifs domain preferred-dc add -vserver vserver_name -
   domain domain_name -preferred-dc IP_address, …+
   ```

   Perintah berikut menambahkan pengontrol domain 172.17.102.25 dan 172.17.102.24 ke daftar pengontrol domain pilihan yang digunakan server SMB di SVM vs1 untuk mengelola akses eksternal ke domain cifs.lab.example.com.

   ```
   FsxId123456789::> vserver cifs domain preferred-dc add -vserver vs1 -domain
    cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
   ```

2. Periksa untuk melihat apakah Pengontrol Domain Anda dapat diselesaikan dengan DNS. Gunakan perintah CLI `vserver services access-check dns forward-lookup` NetApp ONTAP untuk mengembalikan alamat IP nama host berdasarkan pencarian pada server DNS yang ditentukan atau konfigurasi DNS vserver.

   a. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen Amazon fsX NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *`management_endpoint_ip`* dengan alamat IP port manajemen sistem file.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Untuk informasi selengkapnya, lihat Mengelola sistem file dengan ONTAP CLI.

   b. Masukkan mode lanjutan CLI ONTAP menggunakan perintah berikut.

   ```
   FsxId123456789::> set adv
   ```

   c. Masukkan perintah berikut, di mana:

   - `-vserver vserver_name`menentukan nama mesin virtual penyimpanan (SVM).
   - `-hostname host_name`menentukan nama host untuk mencari di server DNS.
   - `-node node_name` menentukan nama node di mana perintah dijalankan.
   - `-lookup-type`menentukan jenis alamat IP yang akan dicari di server DNS, defaultnya adalah. `all`

   ```
   FsxId123456789::> vserver services access-check dns forward-lookup \
   -vserver vserver_name -node node_name \
   -domains domain_name -name-servers dns_server_ip_address \
   -hostname host_name
   ```

3. Tinjau informasi yang perlu Anda miliki saat bergabung dengan SVM ke AD.
4. Tinjau persyaratan jaringan saat bergabung dengan SVM ke AD.
5. Gunakan prosedur yang dijelaskan dalam Persyaratan konfigurasi jaringan untuk memperbarui konfigurasi AD SVM Anda menggunakan alamat IP yang benar untuk server DNS AD Anda.

Amazon FSx tidak dapat berkomunikasi dengan Active Directory karena nama domain Active Directory tidak valid.

Bergabung dengan SVM ke Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

Amazon FSx telah mendeteksi FQDN yang disediakan tidak valid. Untuk memperbaiki masalah ini, perbarui konfigurasi Active Directory mesin virtual penyimpanan Anda dengan FQDN yang mematuhi persyaratan konfigurasi.

Untuk mengatasi masalah ini, gunakan prosedur berikut:

1. Tinjau persyaratan nama domain Active Directory lokal yang dijelaskan dalam Informasi yang dibutuhkan saat bergabung dengan SVM ke Active Directory Pastikan iklan yang Anda coba ikuti memenuhi persyaratan tersebut.
2. Gunakan prosedur yang dijelaskan dalam Bergabung dengan SVM ke Active Directory menggunakan AWS Management Console, AWS CLI dan API dan coba kembali menggabungkan SVM Anda ke AD. Pastikan untuk menggunakan format yang benar untuk FQDN domain AD.

Akun layanan tidak dapat mengakses grup administrator yang ditentukan dalam konfigurasi SVM Active Directory

Bergabung dengan SVM ke Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

Amazon FSx tidak dapat menerapkan konfigurasi Direktori Aktif Anda. Ini karena grup administrator yang Anda berikan tidak ada atau tidak dapat diakses ke akun layanan yang Anda berikan. Untuk memperbaiki masalah ini, pastikan bahwa konfigurasi jaringan Anda memungkinkan lalu lintas dari SVM ke pengontrol domain Active Directory dan server DNS Anda. Kemudian perbarui konfigurasi Direktori Aktif SVM Anda, berikan server DNS Active Directory Anda dan, tentukan grup administrator di domain yang dapat diakses ke akun layanan yang disediakan.

Untuk mengatasi masalah ini, lakukan solusi berikut:

1. Tinjau informasi tentang penyediaan grup domain untuk melakukan tindakan administratif pada SVM Anda. Pastikan Anda menggunakan nama yang benar dari grup administrator domain AD.
2. Gunakan prosedur yang dijelaskan dalam Bergabung dengan SVM ke Active Directory menggunakan AWS Management Console, AWS CLI dan API dan coba kembali menggabungkan SVM Anda ke AD.

Amazon FSx tidak dapat terhubung ke pengontrol domain Direktori Aktif karena unit organisasi yang ditentukan tidak ada atau tidak dapat diakses

Bergabung dengan SVM ke Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

Amazon FSx tidak dapat membuat koneksi dengan Direktori Aktif Anda. Ini karena unit organisasi yang Anda tentukan tidak ada atau tidak dapat diakses oleh akun layanan yang disediakan. Untuk memperbaiki masalah ini, perbarui konfigurasi Active Directory mesin virtual penyimpanan Anda, tentukan unit organisasi tempat akun layanan memiliki izin untuk bergabung.

Untuk mengatasi masalah ini, lakukan solusi berikut:

1. Tinjau prasyarat untuk bergabung dengan SVM ke AD.
2. Tinjau informasi yang perlu Anda miliki saat bergabung dengan SVM ke AD.
3. Coba kembali menggabungkan SVM ke AD menggunakan prosedur ini dengan unit organisasi yang benar.

Anda tidak dapat menghapus penyimpanan mesin virtual atau volume

Setiap FSx untuk sistem file ONTAP dapat berisi satu atau lebih mesin virtual penyimpanan (SVM), dan setiap SVM dapat berisi satu atau lebih volume. Saat Anda menghapus sumber daya, Anda harus terlebih dahulu memastikan bahwa semua anak-anaknya telah dihapus. Misalnya, sebelum menghapus SVM, Anda harus terlebih dahulu menghapus semua volume non-root di SVM.

> **Important**
>
> Anda hanya dapat menghapus penyimpanan mesin virtual dengan menggunakan konsol Amazon FSx, API, dan CLI. Anda hanya dapat menghapus volume menggunakan konsol Amazon FSx, API, atau CLI jika volume telah mengaktifkan cadangan Amazon FSx.

Untuk membantu melindungi data dan konfigurasi Anda, Amazon FSx mencegah penghapusan SVM dan volume dalam keadaan tertentu. Jika Anda mencoba menghapus SVM atau volume, dan permintaan penghapusan Anda tidak berhasil, Amazon FSx memberi Anda informasi di AWS konsol, AWS Command Line Interface (AWS CLI), dan API mengenai alasan sumber daya tidak

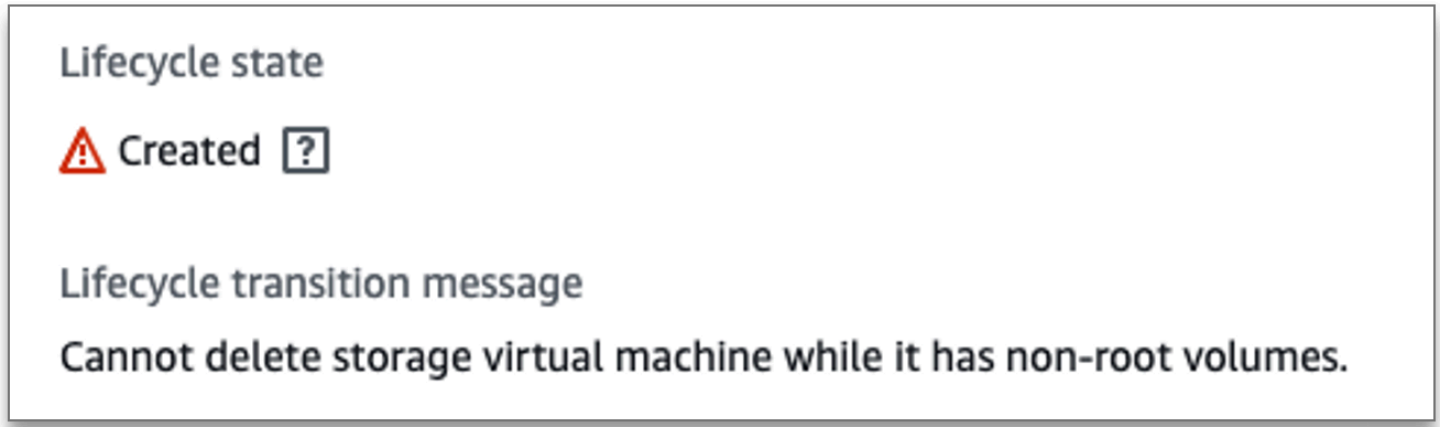
dihapus. Setelah Anda mengatasi penyebab kegagalan penghapusan, Anda dapat mencoba kembali permintaan penghapusan.

Topik

Mengidentifikasi penghapusan yang gagal

Saat menghapus SVM atau volume Amazon FSx, Anda biasanya melihat transisi `Lifecycle` status sumber daya hingga beberapa menit sebelum sumber daya menghilang dari konsol Amazon FSx, CLI, dan API. `DELETING`

Jika Anda mencoba menghapus sumber daya dan transisi `Lifecycle` statusnya dari ke `DELETING` dan kemudian kembali ke`CREATED`, perilaku ini menunjukkan bahwa sumber daya tidak berhasil dihapus. Dalam hal ini, Amazon FSx melaporkan ikon peringatan di konsol di sebelah status Siklus Hidup`CREATED`. Memilih ikon peringatan menampilkan alasan penghapusan yang gagal, seperti yang ditunjukkan pada contoh berikut.



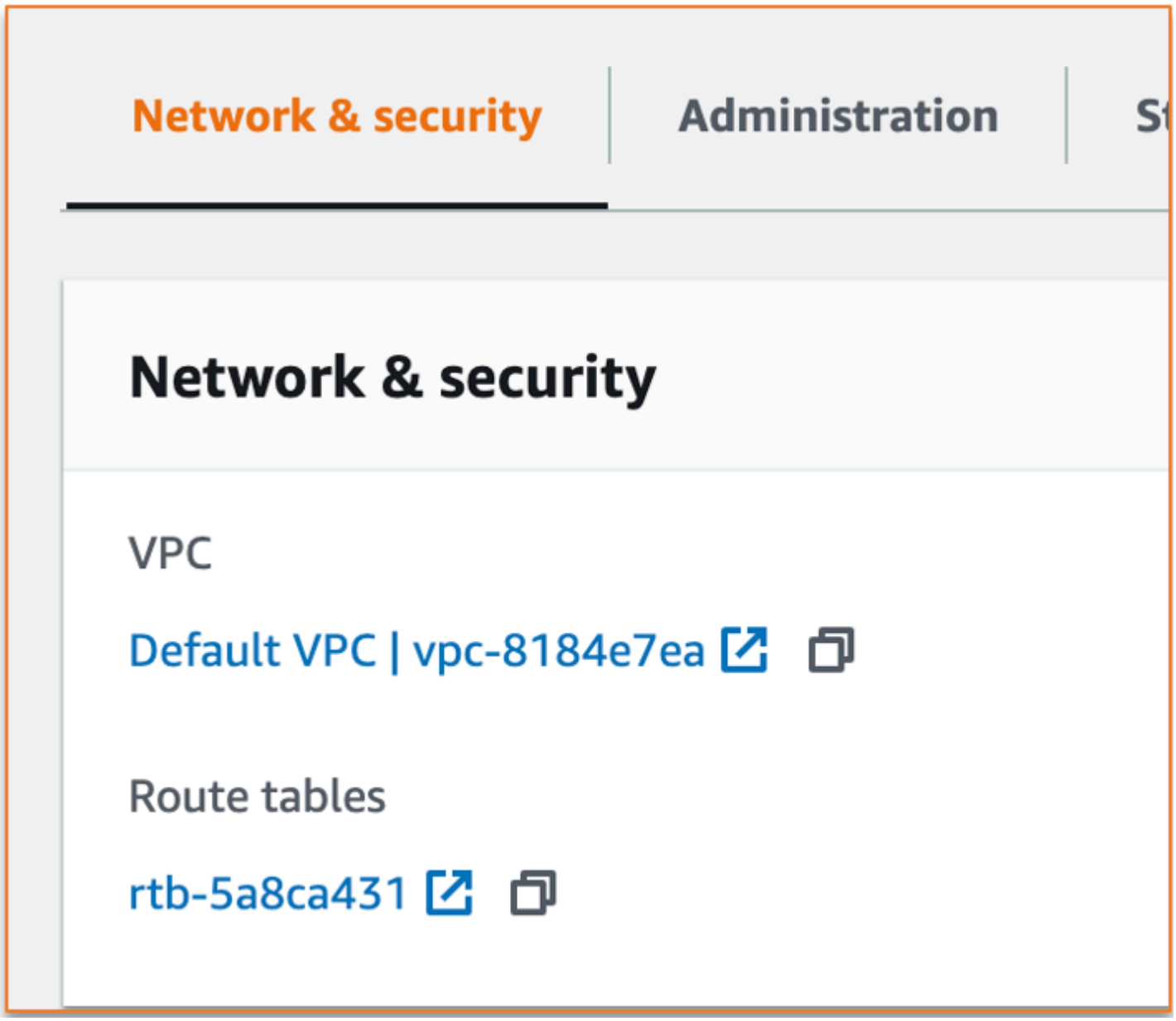
Alasan paling umum mengapa Amazon FSx mencegah SVM dan penghapusan volume disediakan di bagian berikut, dengan step-by-step petunjuk tentang cara mengatasi masalah ini.

Penghapusan SVM: Tabel rute tidak dapat diakses

Setiap fsX untuk sistem file ONTAP membuat satu atau lebih entri tabel rute untuk menyediakan failover otomatis dan gagal kembali di seluruh Availability Zones. Secara default, entri tabel rute ini dibuat di tabel rute default VPC Anda. Anda dapat secara opsional menentukan satu atau lebih tabel rute non-default di mana FSx untuk antarmuka ONTAP dapat dibuat. Amazon FSx menandai setiap tabel rute yang dikaitkan dengan sistem file dengan `AmazonFSx` tag, dan jika tag ini dihapus, itu dapat mencegah Amazon FSx dari dapat menghapus sumber daya. Jika situasi ini terjadi, Anda melihat yang berikut`LifecycleTransitionReason`:

```
Amazon FSx is unable to complete the requested storage virtual machine
operation because of an inability to access one or more of the route tables
associated with your file system. Please contact AWS Support.
```

Anda dapat menemukan tabel rute sistem file Anda di konsol Amazon FSx dengan menavigasi ke halaman ringkasan sistem file, di bawah tab Jaringan & keamanan:



Memilih tautan tabel rute akan membawa Anda ke tabel rute Anda. Selanjutnya, verifikasi bahwa setiap tabel rute yang terkait dengan sistem file Anda ditandai dengan pasangan kunci-nilai ini:

```
Key: AmazonFSx
Value: ManagedByAmazonFSx
```

Jika tag ini tidak ada, buat ulang, lalu coba hapus SVM lagi.

Penghapusan SVM: Hubungan teman sebaya

Jika Anda mencoba menghapus SVM atau volume yang merupakan bagian dari hubungan rekan, Anda harus terlebih dahulu menghapus hubungan rekan sebelum menghapus SVM atau volume. Persyaratan ini mencegah SVM yang diintip menjadi tidak sehat. Jika SVM Anda tidak dapat dihapus karena hubungan teman sebaya, Anda melihat yang berikut ini: `LifecycleTransitionReason`

Amazon FSx tidak dapat menghapus mesin virtual penyimpanan karena merupakan bagian dari hubungan rekan sejawat atau transisi SVM. Harap hapus hubungan dan coba lagi.

Anda dapat menghapus hubungan rekan SVM melalui CLI ONTAP. Untuk mengakses CLI ONTAP, ikuti langkah-langkahnya. Mengelola sistem file dengan ONTAP CLI Menggunakan CLI ONTAP, ambil langkah-langkah berikut.

1. Periksa hubungan rekan SVM dengan menggunakan perintah berikut. Ganti *svm_name* dengan nama SVM Anda.

   ```
   FsxId123456789::> vserver peer show -vserver svm_name
   ```

   Jika perintah ini berhasil, Anda akan melihat output yang mirip dengan berikut ini:

   ```
               Peer        Peer                            Peering        Remote
   Vserver     Vserver     State        Peer Cluster       Applications   Vserver
   ----------- ----------- ------------ ----------------- -------------- ---------
   svm_name    test2       peered       FsxId02d81fef0d84734b6
                                                           snapmirror     fsxDest
   svm_name    test3       peered       FsxId02d81fef0d84734b6
                                                           snapmirror     fsxDest
   ```

```
2 entries were displayed.
```

2. Hapus setiap hubungan rekan SVM dengan menggunakan perintah berikut. Ganti*svm_name*, dan *remote_svm_name* dengan nilai aktual Anda.

```
FsxId123456789abcdef::> vserver peer delete -vserver svm_name -peer-
vserver remote_svm_name
```

Jika perintah ini berhasil, Anda akan melihat output berikut:

```
Info: 'vserver peer delete' command is successful.
```

SVM atau penghapusan volume: SnapMirror

Sama seperti Anda tidak dapat menghapus SVM dengan hubungan rekan tanpa terlebih dahulu menghapus hubungan rekan (lihatPenghapusan SVM: Hubungan teman sebaya), Anda tidak dapat menghapus SVM yang memiliki SnapMirror hubungan tanpa terlebih dahulu menghapus hubungan tersebut. SnapMirror Untuk menghapus SnapMirror hubungan, gunakan ONTAP CLI untuk mengambil langkah-langkah berikut pada sistem file yang menjadi tujuan hubungan. SnapMirror Untuk mengakses CLI ONTAP, ikuti langkah-langkahnya. Mengelola sistem file dengan ONTAP CLI

> **Note**
>
> Cadangan Amazon FSx digunakan SnapMirror untuk membuat point-in-time, cadangan tambahan dari volume sistem file Anda. Anda tidak dapat menghapus SnapMirror hubungan ini untuk cadangan Anda di CLI ONTAP. Namun, hubungan ini secara otomatis dihapus ketika Anda menghapus volume melalui AWS CLI, API, atau konsol.

1. Buat daftar SnapMirror hubungan Anda pada sistem file tujuan dengan menggunakan perintah berikut. Ganti *svm_name* dengan nama SVM Anda.

```
FsxId123456789abcdef::> snapmirror show -vserver svm_name
```

Jika perintah ini berhasil, Anda akan melihat output yang mirip dengan berikut ini:

```
Source            Destination    Mirror  Relationship   Total             Last
Path        Type  Path           State   Status         Progress  Healthy Updated
```

```
----------- ---- ------------    ------- -------------- --------- ------- --------
sourceSvm:sourceVol
            XDP  destSvm:destVol Snapmirrored
                                      Idle           -         true    -
```

2. Hapus SnapMirror hubungan Anda dengan menjalankan perintah berikut pada sistem file tujuan.

```
FsxId123456789abcdef::> snapmirror release -destination-path destSvm:destVol -
source-path sourceSvm:sourceVol -force true
```

Penghapusan SVM: LIF berkemampuan KerberOS

Jika Anda mencoba menghapus SVM yang memiliki antarmuka logis (LIF) dengan Kerberos diaktifkan, Anda harus menonaktifkan Kerberos terlebih dahulu pada LIF itu sebelum menghapus SVM.

Anda dapat menonaktifkan Kerberos pada LIF melalui CLI ONTAP. Untuk mengakses CLI ONTAP, ikuti langkah-langkahnya. Mengelola sistem file dengan ONTAP CLI

1. Masuk ke mode diagnostik di CLI ONTAP dengan menggunakan perintah berikut.

```
FsxId123456789abcdef::> set diag
```

Saat diminta untuk melanjutkan, masukkan**y**.

```
Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y
```

2. Periksa antarmuka mana yang mengaktifkan Kerberos. Ganti *svm_name* dengan nama SVM Anda.

```
FsxId123456789abcdef::> kerberos interface show -vserver svm_name
```

Jika perintah ini berhasil, Anda akan melihat output yang mirip dengan berikut ini:

```
(vserver nfs kerberos interface show)
               Logical
Vserver        Interface     Address         Kerberos SPN
-------------- ------------- --------------- -------- ----------------------
```

```
svm_name        nfs_smb_management_1
                              10.19.153.48    enabled
5 entries were displayed.
```

3. Nonaktifkan LIF Kerberos dengan menggunakan perintah berikut. Ganti *svm_name* dengan nama SVM Anda. Anda harus memberikan nama pengguna dan kata sandi Direktori Aktif yang Anda gunakan untuk menggabungkan SVM ini ke Direktori Aktif Anda.

```
FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
 nfs_smb_management_1
```

Jika perintah ini berhasil, Anda akan melihat output berikut. Berikan nama pengguna dan kata sandi Direktori Aktif yang Anda gunakan untuk menggabungkan SVM ini ke Direktori Aktif Anda. Saat diminta untuk melanjutkan, masukkan**y**.

```
(vserver nfs kerberos interface disable)
Username: admin
Password: *************

Warning: This command deletes the service principal name from the machine account
 on the KDC.
Do you want to continue? {y|n}: y

Disabled Kerberos on LIF "nfs_smb_management_1" in Vserver "svm_name".
```

4. Verifikasi bahwa Kerberos dinonaktifkan pada SVM dengan menggunakan perintah berikut. Ganti *svm_name* dengan nama SVM Anda.

```
FsxId123456789abcdef::> kerberos interface show -vserver svm_name
```

Jika perintah ini berhasil, Anda akan melihat output yang mirip dengan berikut ini:

```
(vserver nfs kerberos interface show)
               Logical
Vserver        Interface     Address         Kerberos SPN
-------------- ------------- --------------- -------- ----------------------
svm_name       nfs_smb_management_1
                             10.19.153.48    disabled
5 entries were displayed.
```

5. Jika antarmuka ditampilkan sebagai`disabled`, coba hapus SVM lagi melalui AWS CLI, API, atau konsol.

   Jika Anda tidak dapat menghapus LIF dengan menggunakan perintah sebelumnya, Anda dapat menghapus paksa LIF Kerberos dengan menggunakan perintah berikut. Ganti *`svm_name`* dengan nama SVM Anda.

   > **Important**
   >
   > Perintah berikut dapat untai objek komputer SVM Anda di Active Directory Anda.

   ```
   FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
    nfs_smb_management_1 -force true
   ```

   Jika perintah ini berhasil, Anda akan melihat output yang mirip dengan berikut ini. Saat diminta untuk melanjutkan, masukkan**y**.

   ```
   (vserver nfs kerberos interface disable)

   Warning: Kerberos configuration for LIF "nfs_smb_management_1" in Vserver
    "svm_name" will be deleted.
   The corresponding account on the KDC will not be deleted. Do you want to continue?
    {y|n}: y
   ```

Penghapusan SVM: Alasan lain

FSx untuk ONTAP SVM membuat objek komputer di Direktori Aktif Anda saat mereka bergabung dengan Direktori Aktif Anda. Dalam beberapa kasus, Anda mungkin ingin secara manual memutuskan sambungan SVM dari Active Directory Anda dengan menggunakan ONTAP CLI. Untuk mengakses CLI ONTAP, ikuti langkah-langkahnya, Mengelola sistem file dengan ONTAP CLI masuk ke CLI ONTAP di tingkat sistem file dengan kredensyal. `fsxadmin` Menggunakan CLI ONTAP, ambil langkah-langkah berikut untuk memutuskan sambungan SVM dari Active Directory Anda.

> **Important**
>
> Prosedur ini dapat untai objek komputer SVM Anda di Active Directory Anda.

1. Masuk ke mode lanjutan di CLI ONTAP dengan menggunakan perintah berikut.

```
FsxId123456789abcdef::> set adv
```

Setelah menjalankan perintah ini, Anda akan melihat output ini. Masuk **y** untuk melanjutkan.

```
Warning: These advanced commands are potentially dangerous; use them only when
      directed to do so by NetApp personnel.
      Do you want to continue? {y|n}: y
```

2. Hapus DNS untuk Active Directory Anda dengan menggunakan perintah berikut. Ganti *svm_name* dengan nama SVM Anda.

```
FsxId123456789abcdef::> vserver services name-service dns dynamic-update record
 delete -vserver svm_name -lif nfs_smb_management_1
```

> **Note**
>
> Jika catatan DNS telah dihapus atau jika server DNS tidak dapat dijangkau, perintah ini gagal. Jika itu terjadi, lanjutkan dengan langkah berikutnya.

3. Nonaktifkan DNS dengan menggunakan perintah berikut. Ganti *svm_name* dengan nama SVM Anda.

```
FsxId123456789abcdef::> vserver services name-service dns dynamic-update modify -
vserver svm_name -is-enabled false -use-secure false
```

Jika perintah ini berhasil, Anda akan melihat output berikut:

```
Warning: DNS updates for Vserver "svm_name" are now disabled.
     Any LIFs that are subsequently modified or deleted
     can result in a stale DNS entry on the DNS server,
     even when DNS updates are enabled again.
```

4. Putuskan sambungan perangkat dari Active Directory. Ganti *svm_name* dengan nama SVM Anda.

```
FsxId123456789abcdef::> vserver cifs delete -vserver svm_name
```

Setelah menjalankan perintah ini, Anda akan melihat output berikut, di *CORP.EXAMPLE.COM* mana diganti dengan nama domain Anda. Saat diminta, masukkan nama pengguna dan kata sandi Anda. Ketika ditanya apakah Anda ingin menghapus server, masukkan**y**.

```
In order to delete an Active Directory machine account for the CIFS server,
you must supply the name and password of a Windows account with sufficient
privileges to remove computers from the "CORP.EXAMPLE.COM" domain.
Enter the user name: admin
Enter the password:
Warning: There are one or more shares associated with this CIFS server
     Do you really want to delete this CIFS server and all its shares? {y|n}: y
Warning: Unable to delete the Active Directory computer account for this CIFS
 server.
     Do you want to continue with CIFS server deletion anyway? {y|n}: y
```

Penghapusan volume: hubungan FlexCache

Anda tidak dapat menghapus volume yang merupakan volume asal untuk suatu FlexCache hubungan kecuali Anda menghapus hubungan cache terlebih dahulu. Untuk menentukan volume mana yang memiliki FlexCache hubungan, Anda dapat menggunakan CLI ONTAP. Untuk mengakses CLI ONTAP, ikuti langkah-langkahnya. Mengelola sistem file dengan ONTAP CLI

1. Periksa FlexCache hubungan dengan menggunakan perintah berikut.

```
FsxId123456789abcdef::> volume flexcache origin show-caches
```

2. Hapus setiap hubungan cache dengan menggunakan perintah berikut. Ganti*dest_svm_name*, dan *dest_vol_name* dengan nilai aktual Anda.

```
FsxId123456789abcdef::> volume flexcache delete -vserver dest_svm_name -
volume dest_vol_name
```

3. Setelah Anda menghapus hubungan cache, coba hapus SVM Anda melalui AWS CLI, API, atau konsol lagi.

Pencadangan harian otomatis gagal karena kapasitas volume yang tidak mencukupi

Pencadangan harian otomatis volume Anda gagal dengan pesan berikut:

```
Amazon FSx could not create a backup of your volume because the backup snapshot was
 deleted.
```

Pencadangan harian otomatis gagal karena kapasitas penyimpanan gratis tidak mencukupi pada volume. Untuk mengurangi kondisi ini, Anda perlu mengosongkan kapasitas penyimpanan pada volume. Anda dapat melakukannya dengan menggunakan satu atau lebih opsi berikut, tergantung pada situasi Anda:

- Meningkatkan kapasitas penyimpanan volume
- Tingkatkan cadangan snapshot volume
- Nonaktifkan penghapusan otomatis snapshot
- Jangan hapus snapshot cadangan menggunakan ONTAP CLI

Anda memiliki kapasitas volume yang tidak mencukupi

Jika Anda kehabisan ruang pada volume Anda, Anda dapat menggunakan prosedur yang ditunjukkan di sini untuk mendiagnosis dan menyelesaikan situasi.

Topik

- Tentukan bagaimana kapasitas penyimpanan volume Anda digunakan
- Meningkatkan kapasitas penyimpanan volume
- Menggunakan autosizing volume
- Penyimpanan utama sistem file Anda penuh
- Menghapus snapshot
- Meningkatkan kapasitas file maksimum volume

Tentukan bagaimana kapasitas penyimpanan volume Anda digunakan

Anda dapat melihat bagaimana kapasitas penyimpanan volume Anda dikonsumsi dengan menggunakan perintah `volume show-space` NetApp ONTAP CLI. Informasi ini dapat membantu

Anda membuat keputusan tentang cara merebut kembali atau menghemat kapasitas penyimpanan volume. Untuk informasi selengkapnya, lihat Untuk memantau kapasitas penyimpanan volume (konsol).

Meningkatkan kapasitas penyimpanan volume

Anda dapat meningkatkan kapasitas penyimpanan volume dengan menggunakan konsol Amazon FSx AWS CLI, dan Amazon FSx API. Untuk informasi lebih lanjut tentang memperbarui volume dengan kapasitas yang meningkat, lihatMemperbarui volume.

Atau, Anda dapat meningkatkan kapasitas penyimpanan volume menggunakan perintah `volume modify` NetApp ONTAP CLI. Untuk informasi selengkapnya, lihat Untuk mengubah kapasitas penyimpanan volume (konsol).

Menggunakan autosizing volume

Anda dapat menggunakan autosizing volume sehingga volume secara otomatis tumbuh dengan jumlah tertentu, atau ke ukuran tertentu ketika mencapai ambang ruang yang digunakan. Anda dapat melakukan ini untuk tipe FlexVol volume, yang merupakan tipe volume default untuk FSx untuk ONTAP, menggunakan perintah ONTAP `volume autosize` NetApp CLI. Untuk informasi selengkapnya, lihat Mengaktifkan autosizing volume.

Penyimpanan utama sistem file Anda penuh

Jika fsX Anda untuk penyimpanan utama sistem file ONTAP penuh, Anda tidak dapat menambahkan data lagi ke volume dalam sistem file Anda, bahkan jika volume menunjukkan bahwa ia memiliki kapasitas penyimpanan yang cukup tersedia. Anda dapat melihat jumlah kapasitas penyimpanan utama yang tersedia di tab Pemantauan & kinerja pada halaman detail sistem file di konsol Amazon FSx. Lihat informasi yang lebih lengkap di Memantau pemanfaatan penyimpanan SSD

Untuk mengatasi masalah ini, Anda dapat meningkatkan ukuran tingkat penyimpanan utama sistem file Anda. Untuk informasi selengkapnya, lihat Memperbarui penyimpanan SSD sistem file dan IOPS.

Menghapus snapshot

Snapshot diaktifkan secara default pada volume Anda, menggunakan kebijakan snapshot default. Snapshot disimpan di `.snapshot` direktori di root volume. Anda dapat mengelola kapasitas penyimpanan volume sehubungan dengan snapshot dengan cara berikut:

- Hapus snapshot secara manual — merebut kembali kapasitas penyimpanan dengan menghapus snapshot secara manual.
- Buat kebijakan penghapusan otomatis snapshot — buat kebijakan yang menghapus snapshot lebih agresif daripada kebijakan snapshot default.
- Matikan snapshot otomatis — hemat kapasitas penyimpanan dengan mematikan snapshot otomatis.

Untuk informasi selengkapnya tentang menghapus snapshot dan mengelola kebijakan snapshot untuk menghemat kapasitas penyimpanan, lihat. Menghapus snapshot

Meningkatkan kapasitas file maksimum volume

FSx untuk volume ONTAP dapat kehabisan kapasitas file ketika jumlah inode yang tersedia, atau pointer file, habis. Secara default, jumlah inode yang tersedia pada volume adalah 1 untuk setiap 32KiB ukuran volume. Untuk informasi selengkapnya, lihat Kapasitas file volume.

Jumlah inode dalam volume meningkat sepadan dengan kapasitas penyimpanan volume, hingga ambang batas 648 GiB. Secara default, volume yang memiliki kapasitas penyimpanan 648 GiB atau lebih semuanya memiliki jumlah inode yang sama, 21.251.126. Untuk melihat kapasitas file maksimum volume, lihatMelihat kapasitas file volume.

Jika Anda membuat volume lebih besar dari 648 GiB, dan Anda ingin memiliki lebih dari 21.251.126 inode, Anda harus meningkatkan jumlah maksimum file pada volume secara manual. Jika volume Anda kehabisan kapasitas penyimpanan, Anda dapat memeriksa kapasitas file maksimumnya. Jika mendekati kapasitas filenya, Anda dapat meningkatkannya secara manual. Untuk informasi selengkapnya, lihat Untuk meningkatkan jumlah maksimum file pada volume (ONTAPCLI).

Memecahkan masalah jaringan

Jika Anda mengalami masalah jaringan, Anda dapat menggunakan prosedur yang ditampilkan di sini untuk mendiagnosis masalah.

Anda ingin menangkap jejak paket

Packet tracing adalah proses memverifikasi jalur paket melalui lapisan ke tujuannya. Anda mengontrol proses pelacakan paket dengan perintah CLI NetApp ONTAP berikut:

- network tcpdump start— Memulai penelusuran paket
- network tcpdump show— Menunjukkan jejak paket yang sedang berjalan
- network tcpdump stop— Menghentikan jejak paket yang sedang berjalan

Perintah ini tersedia untuk pengguna yang memiliki `fsxadmin` peran pada sistem file Anda.

Untuk menangkap jejak paket dari sistem file Anda

1. Untuk SSH ke NetApp CLI ONTAP sistem file Anda, ikuti langkah-langkah yang didokumentasikan di bagian Panduan Pengguna Amazon FSx untuk ONTAP. Menggunakan CLI NetApp ONTAP NetApp

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Masukkan tingkat hak istimewa diagnostik di CLI ONTAP dengan menggunakan perintah berikut.

   ```
   ::> set diag
   ```

   Saat diminta untuk melanjutkan, masukkany.

   ```
   Warning: These diagnostic commands are for use by NetApp personnel only.
   Do you want to continue? {y|n}: y
   ```

3. Identifikasi lokasi pada sistem file Anda di mana Anda ingin menyimpan jejak paket Anda. Volume harus online dan harus dipasang di namespace dengan jalur persimpangan yang valid. Gunakan perintah berikut untuk memeriksa volume yang memenuhi kriteria tersebut:

   ```
   ::*> volume show -junction-path !- -fields junction-path
   vserver volume    junction-path
   ------- --------- -------------
   fsx     test_vol1 /test_vol1
   fsx     test_vol2 /test_vol2
   fsx     test_vol2 /test_vol3
   ```

4. Mulai jejak dengan argumen minimum yang diperlukan. Ganti yang berikut ini:

   - Ganti *node_name* dengan nama node (misalnya,). `FsxId01234567890abcdef-01`
   - Ganti *svm_name* dengan nama mesin virtual penyimpanan Anda (misalnya,). `fsx`
   - Ganti *junction_path_name* dengan nama volume (misalnya,). `test-vol1`

```
::*> debug network tcpdump start -node node_name -ipspace Default -pass-through "-i
 e0e -w /clus/svm_name/junction_path_name"
Info: Started network trace on interface "e0e"
Warning: Snapshots should be disabled on the tcpdump destination volume while
 packet traces are occurring. Use the
"volume modify -snapshot-policy none -vserver fsx -volume test_vol1" command to
 disable Snapshots on the
tcpdump destination volume.
```

> **Important**
>
> Jejak paket hanya dapat ditangkap pada `e0e` antarmuka dan di ruang `Default` IP. Di FSx untuk ONTAP, semua lalu lintas jaringan menggunakan antarmuka. `e0e`

Saat menggunakan packet tracing, ingatlah hal berikut:

- *Saat memulai jejak paket, Anda harus menyertakan jalur ke tempat Anda ingin menyimpan file jejak, dalam format ini: /clus/svm_name/junction-path-name*
- Secara opsional, berikan nama file untuk jejak paket. *Jika filter_name tidak ditentukan, secara otomatis dihasilkan dalam bentuk: node-name _ port-name _ yyyymmdd_hhmmss .trc*
- Jika jejak bergulir ditentukan, filter_name diakhiran dengan angka yang menunjukkan posisi dalam urutan rotasi.
- CLI ONTAP juga menerima argumen opsional berikut: -pass-through

```
-B, --buffer-size=<KiB>
-c <number_of_packets>
-C <file_size-mB>
-F <filter_expression_filename>
-G <rotate_seconds>
--time-stamp-precision {micro|nano}
-Q, --direction {in|out|inout}
-s, --snapshot-length=<bytes>
-U, --packet-buffered
-W <rotate_file_count>
```

```
<filter-expression>
```

- Untuk informasi tentang ekspresi filter, lihat halaman manual pcap-filter (7).

5. Lihat jejak yang sedang berlangsung:

```
::*> debug network tcpdump show
Node                    IPspace  Port     Filename
----------------------  -------- -------- --------
FsxId123456789abcdef-01  Default  e0e      /clus/fsx/test_vol1/
FsxId123456789abcdef-01_e0e_20230605_181451.trc
```

6. Hentikan jejaknya:

```
::*> debug network tcpdump stop -node FsxId123456789abcdef-01 -ipspace Default -
port e0e
Info: Stopped network trace on interface "e0e"
```

7. Kembali ke tingkat hak istimewa admin:

```
::*> set -priv admin
::>
```

8. Akses jejak paket.

   Jejak paket Anda disimpan dalam volume yang Anda tentukan menggunakan debug network tcpdump start perintah, dan dapat diakses melalui ekspor NFS atau berbagi SMB yang sesuai dengan volume itu.

Untuk informasi selengkapnya tentang menangkap jejak paket, lihat Cara menggunakan tcpdump jaringan debug di ONTAP 9.10+ di Pangkalan Pengetahuan. NetApp

Riwayat Dokumen untuk Amazon FSx untuk ONTAP NetApp

- Versi API: 2018-03-01
- Pembaruan dokumentasi terbaru: 30 April 2024

Tabel berikut menjelaskan perubahan penting pada Panduan Pengguna Amazon FSx NetApp ONTAP. Untuk notifikasi tentang pembaruan dokumentasi, Anda dapat berlangganan ke umpan RSS.

Perubahan	Deskripsi	Tanggal
Support ditambahkan untuk `fsxadmin-readonly` peran bagi pengguna administrasi sistem file	`fsxadmin-readonly` Peran ini sekarang tersedia untuk pengguna administrasi sistem ONTAP file, dan dapat digunakan untuk aplikasi pemantauan sistem file sepertiNetApp Harvest. Untuk informasi selengkapnya, lihat Peran dan pengguna administrator sistem berkas.	April 30, 2024
Support ditambahkan untuk otentikasi kunci publik SSH untuk pengguna administratif domain Windows	Anda sekarang dapat menggunakan otentikasi kunci publik SSH dengan sistem file domain Active Directory dan pengguna SVM. Untuk informasi selengkapnya, lihat https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/set-up-ad-auth.html.	April 30, 2024
Support ditambahkan untuk 12 pasangan HA dalam sistem file scale-out	Amazon FSx untuk NetApp ONTAP menambahkan dukungan untuk 12 pasangan HA dalam sistem file scale-out . Sistem file dengan 12 pasang	Maret 4, 2024

	HA dapat menghasilkan kapasitas throughput hingga 72 GBps dan 2.400.000 IOPS SSD di 12 pasangan ketersediaan tinggi (HA). Untuk informasi selengkapnya, lihat Pasangan ketersediaan tinggi (HA) dan Amazon FSx NetApp untuk kinerja ONTAP.	
Support ditambahkan untuk mode tulis cloud	Amazon FSx untuk NetApp ONTAP menambahkan dukungan untuk mode tulis cloud untuk volume. Untuk informasi selengkapnya, lihat Mengaktifkan mode tulis cloud pada volume.	Februari 6, 2024
Support ditambahkan untuk membuat cadangan FlexGroup volume dengan AWS Backup	Anda sekarang dapat menggunakan AWS Backup untuk mencadangkan dan mengembalikan FlexGroup volume pada FSx Anda untuk sistem file ONTAP. Untuk informasi selengkapnya, lihat Menggunakan AWS Backup dengan Amazon FSx.	Januari 11, 2024

Amazon FSx memperbarui kebijakan terkelola AmazonF, AmazonFSxFullAccess, AmazonFSxConsoleFullAccess, dan SxReadOnlyAccess AmazonF SxConsoleReadOnlyAccess SxServiceRolePolicy AWS	Amazon FSx memperbarui kebijakan AmazonF, AmazonFSxFullAccess, AmazonF, AmazonFSx ConsoleFullAccess, dan AmazonF SxReadOnlyAccess untuk menambahkan SxConsoleReadOnlyAccess izin. SxServiceRolePolicy `ec2:GetSecurityGroupsForVpc` Untuk informasi selengkapnya, lihat Amazon FSx memperbarui kebijakan AWS terkelola.	Januari 9, 2024
Amazon FSx memperbarui kebijakan terkelola AmazonF SxFullAccess dan AmazonF SxConsoleFullAccess AWS	Amazon FSx memperbarui kebijakan AmazonF SxFullAccess dan AmazonF SxConsoleFullAccess untuk menambahkan tindakan. `ManageCrossAccountDataReplication` Untuk informasi selengkapnya, lihat Amazon FSx memperbarui kebijakan AWS terkelola.	20 Desember 2023
Support ditambahkan untuk metrik scale-out	FSx untuk ONTAP sekarang menyediakan CloudWatch metrik Amazon untuk sistem file dengan beberapa pasangan HA. Untuk informasi selengkapnya, lihat Metrik sistem file Scale-out.	26 November 2023

Support ditambahkan untuk sistem file scale-out	Amazon FSx untuk NetApp ONTAP menambahkan dukungan untuk sistem file scale-out yang dapat memberikan kapasitas throughput hingga 36 GBps dan 1.200.000 IOPS SSD di enam pasangan ketersediaan tinggi (HA). Untuk informasi selengkapnya, lihat Pasangan ketersediaan tinggi (HA) dan Amazon FSx NetApp untuk kinerja ONTAP.	26 November 2023
Support ditambahkan untuk FlexGroup volume	Amazon FSx untuk NetApp ONTAP menambahkan dukungan untuk volume. FlexGroup Untuk informasi selengkapnya, lihat Gaya volume.	26 November 2023
Dukungan VPC bersama ditambahkan untuk sistem file Multi-AZ	Akun peserta sekarang dapat membuat sistem file multi-AZ dalam VPC yang telah dibagikan dengan mereka. Akun pemilik dapat mengelola fitur ini di konsol Amazon FSx, CLI, dan API. Untuk informasi selengkapnya, lihat Membuat FSx untuk sistem file ONTAP di subnet bersama	26 November 2023

Amazon FSx memperbarui kebijakan terkelola AmazonFSxFullAccess dan AmazonFSxConsoleFullAccess AWS	Amazon FSx memperbarui kebijakan AmazonFSxFullAccess dan AmazonFSxConsoleFullAccess untuk menambahkan izin. `fsx:CopySnapshotAndUpdateVolume` Untuk informasi selengkapnya, lihat Amazon FSx memperbarui kebijakan AWS terkelola.	26 November 2023
Amazon FSx memperbarui kebijakan terkelola AmazonFSxFullAccess dan AmazonFSxConsoleFullAccess AWS	Amazon FSx memperbarui SxConsoleFullAccess kebijakan AmazonF dan AmazonF untuk menambahkan SxFullAccess dan izin. `fsx:DescribeSharedVPCConfiguration` `fsx:UpdateSharedVPCConfiguration` Untuk informasi selengkapnya, lihat Amazon FSx memperbarui kebijakan AWS terkelola.	14 November 2023
Support ditambahkan untuk membuat peran dan pengguna ONTAP tambahan	Amazon FSx untuk NetApp ONTAP sekarang mendukung pembuatan peran ONTAP tambahan dan pengguna untuk menentukan kemampuan dan hak istimewa pengguna saat menggunakan ONTAP CLI dan REST API. Untuk informasi selengkapnya, lihat Peran dan pengguna di Amazon FSx untuk NetApp ONTAP.	September 6, 2023

Support ditambahkan untuk CloudWatch metrik tambahan dan dasbor pemantauan yang disempurnakan	FSx untuk ONTAP sekarang menyediakan metrik kinerja tambahan dan dasbor pemantauan yang disempurnakan untuk meningkatkan visibilitas ke dalam aktivitas sistem file. Untuk informasi lebih lanjut, lihat Memantau dengan CloudWatch.	17 Agustus 2023
Amazon FSx memperbarui kebijakan terkelola SxService RolePolicy AWS AmazonF	Amazon FSx memperbarui `cloudwatch:PutMetricData` izin di AmazonF. SxServiceRolePolicy Untuk informasi selengkapnya, lihat Amazon FSx memperbarui kebijakan AWS terkelola.	Juli 24, 2023
Support ditambahkan untuk menggunakan NetApp System Manager secara langsung	Anda dapat mengelola FSx Anda untuk sistem file ONTAP menggunakan System Manager langsung dari. NetApp BlueXP Untuk informasi selengkapnya, lihat Menggunakan Manajer NetApp Sistem dengan BlueXP.	13 Juli 2023

Support ditambahkan untuk memantau acara EMS	Anda dapat memantau FSx untuk peristiwa sistem file ONTAP menggunakan asli NetApp ONTAP. Events Management System (EMS) Anda dapat melihat acara EMS menggunakan CLI NetApp ONTAP. Untuk informasi selengkapnya, lihat Memantau FSx untuk acara ONTAP EMS.	13 Juli 2023
Support ditambahkan untuk SnapLock	FSx untuk ONTAP sekarang mendukung volume. SnapLock SnapLockmemungkinkan Anda untuk melindungi file Anda dengan mentransi sisinya ke status tulis sekali, baca banyak (WORM), yang mencegah modifikas i atau penghapusan untuk periode retensi tertentu. FSx untuk ONTAP mendukung mode Kepatuhan dan retensi Perusahaan dengan. SnapLock Untuk informasi lebih lanjut, lihat Bekerja dengan SnapLock.	13 Juli 2023

Support ditambahkan untuk enkripsi IPsec data dalam perjalanan	FSx untuk ONTAP sekarang mendukung penggunaan enkripsi IPsec untuk mengenkripsi data dalam perjalanan antara sistem file dan klien yang terhubung. Untuk informasi selengkapnya, lihat Mengonfigurasi IPSec menggunakan otentikasi PSK dan Mengonfigurasi IPSec menggunakan otentikasi sertifikat.	13 Juli 2023
Ukuran volume maksimum telah meningkat	FSx untuk ONTAP memperbarui ukuran maksimum volume dari 100 TB menjadi 300 TB. Untuk informasi selengkapnya, lihat Mengaktifkan autosizing volume.	13 Juli 2023
Amazon FSx memperbarui kebijakan terkelola SxFullAccess AWS AmazonF	Amazon FSx memperbarui SxFullAccess kebijakan AmazonF untuk menghapus `fsx:*` izin dan menambahkan tindakan tertentu. `fsx` Untuk informasi selengkapnya, lihat kebijakan AmazonF SxFullAccess.	13 Juli 2023

Amazon FSx memperbarui kebijakan terkelola SxConsole FullAccess AWS AmazonF	Amazon FSx memperbarui SxConsoleFullAccess kebijakan AmazonF untuk menghapus `fsx:*` izin dan menambahkan tindakan tertentu. `fsx` Untuk informasi selengkapnya, lihat kebijakan AmazonF SxConsoleFullAccess.	13 Juli 2023
Support ditambahkan untuk menggabungkan mesin virtual penyimpanan yang ada ke Active Directory	Anda dapat menggabungkan mesin virtual penyimpanan yang ada ke Active Directory menggunakan AWS Management Console, AWS CLI dan API. Untuk informasi selengkapnya, lihat Menggabungkan SVM ke Direktori Aktif.	13 Juni 2023
Support untuk cache baca NVMe ditambahkan untuk sistem file Single-AZ	Cache baca NVMe sekarang didukung untuk sistem file AZ tunggal yang dibuat setelah 28 November 2022 dengan setidaknya 2 GBps kapasitas throughput di Wilayah AS Timur (Ohio), Wilayah AS Timur (Virginia N.), Wilayah AS Barat (Oregon), dan Eropa (Irlandia). Untuk informasi selengkapnya, lihat Dampak jenis penerapan pada performa.	28 November 2022

Support ditambahkan untuk menggunakan rentang alamat IP in-vPC untuk membuat sistem file multi-AZ	Anda sekarang dapat membuat Multi-AZ FSx untuk sistem file ONTAP dengan menentukan titik akhir yang berada dalam rentang alamat IP VPC Anda. Untuk informasi selengkapnya, lihat Membuat FSx untuk sistem file ONTAP.	28 November 2022
Support ditambahkan untuk memperbarui tabel rute VPC pada sistem file Multi-AZ	Anda sekarang dapat mengaitkan (menambah kan) tabel rute VPC baru ke FSx Multi-AZ untuk sistem file ONTAP yang ada atau memisahkan (menghapus) tabel rute VPC yang ada dari FSX multi-AZ yang ada untuk sistem file ONTAP. Untuk informasi selengkapnya, lihat Memperbarui sistem file.	28 November 2022
Support ditambahkan untuk enkripsi data dalam perjalanan dengan AWS Nitro System	Data dalam perjalanan dienkripsi secara otomatis ketika diakses dari instans Amazon EC2 yang didukung di Wilayah AS Timur (Ohio), Wilayah AS Timur (Virginia N.), Wilayah AS Barat (Oregon), dan Eropa (Irlandia). Untuk informasi selengkapnya, lihat Mengenkripsi data dalam perjalanan dengan Sistem AWS Nitro.	28 November 2022

Support ditambahkan untuk membuat volume DP	Anda sekarang dapat membuat volume DP (perlindungan data) dengan menggunakan konsol Amazon FSx,, atau AWS CLI Amazon FSx API. Anda dapat menggunakan volume DP sebagai tujuan SnapVault hubungan NetApp SnapMirro r atau, saat Anda ingin memigrasi atau melindung i data satu volume. Untuk informasi selengkapnya, lihat Jenis volume.	28 November 2022
Support ditambahkan untuk menyalin tag volume ke backup	Anda sekarang dapat mengaktifkan `CopyTagsT oBackups` di AWS CLI atau Amazon FSx API untuk secara otomatis menyalin tag dari volume Anda ke backup. Untuk informasi selengkap nya, lihat Menyalin tag ke cadangan.	28 November 2022

Support ditambahkan untuk memilih kebijakan snapshot	Sekarang Anda dapat memilih dari tiga kebijakan snapshot bawaan saat membuat atau memperbarui volume menggunakan konsol Amazon FSx AWS CLI,, atau Amazon FSx API. Anda juga dapat memilih kebijakan snapshot khusus yang dibuat di ONTAP CLI atau REST API. Untuk informasi selengkapnya, lihat Kebijakan snapshot.	28 November 2022
Support ditambahkan untuk opsi kapasitas throughput sistem file tambahan	FSx untuk ONTAP sekarang mendukung 4.096 MBps kapasitas throughput untuk sistem file yang dibuat setelah 28 November 2022 di Wilayah AS Timur (Ohio), Wilayah AS Timur (Virginia N.), Wilayah AS Barat (Oregon), dan Eropa (Irlandia). Untuk informasi selengkapnya, lihat Dampak kapasitas throughput terhadap kinerja.	28 November 2022

Support ditambahkan untuk IOPS SSD tambahan	FSx untuk ONTAP sekarang mendukung 160.000 IOPS SSD untuk sistem file yang dibuat setelah 28 November 2022 di Wilayah AS Timur (Ohio), Wilayah AS Timur (Virginia N.), Wilayah AS Barat (Oregon), dan Eropa (Irlandia). Untuk informasi selengkap nya, lihat Dampak kapasitas throughput terhadap kinerja.	28 November 2022
Support ditambahkan untuk menggunakan FSx untuk ONTAP sebagai datastore eksternal untuk VMware Cloud on AWS	Anda dapat menggunakan FSx untuk ONTAP sebagai datastore eksternal untuk VMware Cloud pada AWS Pusat Data yang Ditetapka n Perangkat Lunak (SDDC). Dukungan tambahan ini memberikan fleksibilitas untuk meningkatkan atau menurunka n penyimpanan secara independen dari sumber daya komputasi untuk VMware Cloud pada beban kerja. AWS Untuk informasi selengkapnya, lihat Menggunakan VMware Cloud dengan FSx untuk ONTAP.	30 Agustus 2022

Secara otomatis meningkatkan kapasitas penyimpanan sistem file	Gunakan AWS CloudFormation template AWS yang dapat disesuaikan yang dikembangkan untuk secara otomatis meningkatkan kapasitas penyimpanan sistem file Anda ketika jumlah kapasitas penyimpanan SSD yang digunakan melebihi ambang batas yang Anda tentukan. Untuk informasi selengkapnya, lihat Meningkatkan kapasitas penyimpanan SSD secara dinamis.	Juni 3, 2022
Amazon FSx sekarang terintegrasi dengan AWS Backup	Anda sekarang dapat menggunakan AWS Backup untuk mencadangkan dan memulihkan sistem file FSx Anda selain menggunakan cadangan Amazon FSx asli. Untuk informasi selengkapnya, lihat Menggunakan AWS Backup dengan Amazon FSx.	Mei 18, 2022
Support ditambahkan untuk penyebaran sistem file ONTAP Zona Ketersediaan tunggal	Anda dapat membuat FSx single-AZ untuk sistem file ONTAP, yang dirancang untuk memberikan ketersediaan dan daya tahan tinggi dalam satu Availability Zone (AZ). Untuk informasi selengkapnya, lihat Memilih penerapan sistem file.	13 April 2022

Support ditambahkan untuk titik AWS PrivateLink akhir VPC antarmuka	Anda sekarang dapat menggunakan titik akhir VPC antarmuka untuk mengakses Amazon FSx API dari VPC Anda tanpa mengirim lalu lintas melalui internet. Untuk informasi selengkapnya, lihat Amazon FSx dan titik akhir VPC antarmuka.	5 April 2022
Support ditambahkan untuk memodifikasi kapasitas throughput untuk sistem file ONTAP yang ada	Anda sekarang dapat memodifikasi kapasitas throughput yang tersedia untuk sistem file ONTAP yang ada. Untuk informasi selengkapnya, lihat Mengelola kapasitas throughput.	Maret 30, 2022
Support ditambahkan untuk kapasitas penyimpanan SSD dan penskalaan IOPS yang disediakan	Anda sekarang dapat meningkatkan kapasitas penyimpanan SSD dan IOPS yang disediakan untuk FSx yang ada untuk sistem file ONTAP saat penyimpanan dan persyaratan IOPS Anda berkembang. Untuk informasi selengkapnya, lihat Mengelola kapasitas penyimpanan dan IOPS yang disediakan.	Januari 25, 2022

Support ditambahkan untuk CloudWatch metrik Amazon	Anda dapat memantau sistem file Anda menggunakan Amazon CloudWatch, yang mengumpulkan dan memproses data mentah dari FSx untuk ONTAP menjadi metrik yang dapat dibaca, mendekati waktu nyata. Untuk informasi selengkapnya, lihat Memantau dengan Amazon CloudWatch.	Januari 19, 2022
Support ditambahkan untuk opsi throughput sistem file tambahan	FSx untuk ONTAP sekarang mendukung opsi 128 MB/s dan 256 MB/s untuk throughput sistem file. Untuk informasi selengkapnya, lihat Dampak kapasitas throughput terhadap kinerja.	30 November 2021
Amazon FSx untuk NetApp ONTAP sekarang tersedia secara umum	FSx untuk ONTAP adalah layanan yang dikelola sepenuhnya yang menyediakan penyimpanan file yang sangat andal, terukur, berkinerja, dan kaya fitur yang dibangun di atas sistem file ONTAP. NetApp Ini menyediakan fitur, kinerja, kemampuan, dan API sistem NetApp file yang sudah dikenal dengan kelincahan, skalabilitas, dan kesederhanaan layanan yang dikelola AWS sepenuhnya.	2 September 2021

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.